PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	10/674,929
Filing Date:	September 30, 2003
Applicant:	Rodney B. Kendrick
Group Art Unit:	3626
Examiner:	Sheetal Rangrej
Title:	System of Charging for Automobile Insurance
Confirmation No.:	5150
Attorney Docket:	7784-000652

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

(RESUBMISSION)
APPEAL BRIEF
UNDER 37 C.F.R. § 41.37

Madam:

In response to the Notification of Non-Compliant Appeal Brief mailed September 25, 2008, Applicant respectfully re-submits an appeal brief in accordance with 37 C.F.R. § 41.37. This appeal brief is in support of an appeal taken from the January 30, 2008, final rejection of Claims 1, 4, 5, 9, 10, 14, 15, 16, 19, 20, 23, 24 and 28-34. The Notice of Appeal was filed May 28, 2008, and was accompanied by the fee set forth in 37

C.F.R. § 41.20(b)(1). A fee, in accordance with 37 C.F.R. § 41.20(b)(2), is included herewith for the filing of this Appeal Brief.

In accordance with 37 C.F.R. § 41.37(c)(1), the required items with appropriate headings in the order indicated by 37 C.F.R. § 41.37(c)(1)(i) through § 41.37(c)(1)(x) are provided below.

1. REAL PARTY IN INTEREST – UNDER 37 C.F.R. § 41.37(c)(1)(i)

The Boeing Company, being the assignee of the present application, is the real party in interest. *See Reel 014564 and Frame 0741.*

2. RELATED APPEALS & INTERFERENCES - UNDER 37 C.F.R. § 41.37(c)(1)(ii)

To the best of Applicant's knowledge, no other appeals or interferences are pending which will directly affect, be directly affected by or have a bearing on the Board's decision in the present pending appeal.

3. STATUS OF THE CLAIMS – UNDER 37 C.F.R. § 41.37(c)(1)(iii)

On May 28, 2008, Applicant appealed the final rejection of Claims 1, 4, 5, 9, 10, 14, 15, 16, 19, 20, 23, 24 and 28-34 under 35 U.S.C. § 103(a) as being unpatentable over Nakagawa, et al. in view of Wright and further view of McMillan et al. Claims 2, 3, 6, 7, 8, 11, 12, 13, 17, 18, 21, 22, 25, 26 and 27 have been canceled without prejudice to or disclaimer of the subject matter contained therein. No other claim status is applicable.

4. STATUS OF AMENDMENTS – UNDER 37 C.F.R. § 41.37(c)(1)(iv)

No amendment to the claims has been filed or is pending subsequent to the entry of the final rejection.

5. SUMMARY OF THE CLAIMED SUBJECT MATTER – UNDER 37 C.F.R. § 41.37(c)(1)(v)

In accordance with 37 C.F.R. § 41.37(c)(1)(v), the following is a concise explanation of the subject matter defined in each of the independent claims (i.e., Claims 1, 16 and 30). It should be noted that the application as filed did not contain line numbers so for the convenience of the Board a copy of the application imaged with line numbers is included in the Evidence Appendix as Exhibit 5.

None of the claims are drafted, as permitted by 35 U.S.C. § 112, paragraph six and, as such, no further explanation pursuant to 37 C.F.R. § 41.37(c)(1)(v) is included.

To provide a concise explanation of the subject matter defined in each of the independent claims, portions of the application have been appended below to provide examples of the present teachings and the invention as defined in the claims. Citations to the application as originally filed follow each paragraph below. To make reference to the application easier and to comply with the literal wording of 37 C.F.R. § 41.37(c)(1)(v), Applicant includes a copy of the application imaged with page numbers included in the Evidence Appendix as Exhibit 5.

Independent Claims 1, 4, 5, 9, 10, 14, 15, 16, 19, 20, 23, 24 and 28-34

[0014] With reference to FIG. 1, an insurance cost computation system is generally indicated by reference numeral 10. A user 12 operates a vehicle 14 that is either required to be covered by insurance, or for which the user has chosen to purchase insurance coverage. The user 12 contacts a contracting company 16 for example, an automobile insurance company, and elects a pay as you go insurance plan. A computation device 18 can be installed in the vehicle 14. The computation device 18 may establish a communication link with the contracting company 16, and with an external location identification system 20. The computation device 18 monitors the real time location of the vehicle 14 and determines a cost for the vehicle insurance. This cost is transmitted to the contracting company 16 for later billing to the user 12. *See Application at Pg. 5, Ln. 12-25.*

[0015] The computation device 18 may transmit cost information to the contracting company 16 for later billing to the user 12 at various time increments. A user interface 22 is available for the user 12 to contact the contracting company 16 and monitor the cost of the vehicle insurance whenever needed. The computation device 18 only transmits the cost information to the contracting company 16; as such, the user interface 22 will only display the cost of the automobile insurance for the given time increment. *See Application at Pg. 6, Ln. 1-9 (emphasis added).*

[0016] The computation device 18 may also establish communication with the external location identification system 20. The external location identification system 20 transmits information to the computation device 18 from which the computation device

18 may determine the location of the vehicle 14. The location of the vehicle 14, among other factors, is used to compute the cost of the automobile insurance for the given time increment. *See Application at Pg. 6, Ln. 12-18.*

[0017] With reference to FIG. 2, a more detailed view of the computation device 18 is shown along with the various systems that may communicate with the computation device 18. The computation device 18 includes an internal location identification system 24 that receives information from the external location identification system 20 via electromagnetic wave signals such as from a plurality of global positioning system satellites. The internal location identification system 24 determines the geographical location of the car and correlates that information with a cost lookup database 26. The location information is then encrypted and stored in an encrypted location data system 32. Cost information is tallied by a cost calculation system 28, and then sent to a billing transmission system 30 for eventual transmission of the cost information or a cost increment to the contracting company 16. *See Application at Pg. 6, Ln. 19 – Pg. 7, Ln. 8.*

[0020] The cost increment is determined by evaluating the location information and the vehicle information along with the cost lookup database 26. The location information and the vehicle information may take the form of a single variable or a plurality of variables with certain values determined by the vehicle and where the vehicle travels. The plurality of variables is ultimately correlated with the cost lookup database 26. In addition, the plurality of variables may comprise absolute mileage,

hours driven, multipliers associated with geographic indicators, vehicle indicators, or combinations and derivations thereof. *See Application at Pg. 8, Ln. 5-13.*

[0022] The cost increment is sent to the cost calculation system 28. The cost increment, therefore, is defined as an amount of money or, put another way, contains only monetary information. More notably, the cost increment excludes any of the location information or the vehicle information. *See Application at Pg. 8, Ln. 20-23 (emphasis added).*

[0023] The location information and the vehicle information, which are used to derive the cost increment, are saved in the encrypted location data system 32. The cost increment, being only a dollar amount, is passed to the billing transmission system 30, which sends the cost increment to the contracting company 16. *See Application at Pg. 9, Ln. 3-7 (emphasis added).*

[0025] As noted earlier, no location information is transmitted to the contracting company 16 on a regular basis. Situations may arise, however, where review of the location information is necessary, such as for billing disputes. Access to the encrypted location data system 32 and subsequent decryption is possible through a dispute access system 36. It should be appreciated that the dispute access system 36 may be configured in many different ways. Preferably, however, access to the dispute access system 36 only provides access to unencrypted location information when a user password 38 from the user 12 is combined with a contracting company password 34 from the contracting company 16. As such, the only way to decrypt or gain access to the stored location information in the encrypted location data system 32 is with access

by a passkey containing at least both passwords 38 and 34. *See Application at Pg. 9, Ln. 20 – Pg. 10, Ln. 7 (emphasis added).*

[0028] Because the user 12 is able to access the cost increment or cost information through the user interface 22, the user is able to alter use and activity of the vehicle 14 to possibly reduce the cost of the vehicle insurance. The ability to access the cost of the vehicle insurance on a daily basis empowers the vehicle owner to alter driving habits accordingly, which may result in a savings due to changes in vehicle insurance cost. *See Application at Pg. 11, Ln. 10-15.*

[0029] It will be appreciated that the computation device 18 has a single input which may take the form of information from the external location identification system 20, and a single output which is cost information transmitted from the billing transmission system 30 to the contracting company 16. Only when the user 12 and the contracting company 16 utilize the dispute access system 36 with both passwords 38 and 34 is additional communication with the computation device 18 realized. *See Application at Pg. 11, Ln. 21 – Pg. 12, Ln. 21 (emphasis added).*

[0030] As noted above, access to the computation device through the dispute access system 36 is the only way to obtain unencrypted location information from the computation device 18. Because only cost information is transmitted from the computation device 18, privacy concerns surrounding real time location of the vehicle are accommodated as the computation device 18 only transmits a dollar amount. *See Application at Pg. 12, Ln. 3-8 (emphasis added).*

6. *GROUNDS FOR REJECTION TO BE REVIEWED ON APPEAL – UNDER 37 C.F.R. § 41.37(c)(1)(vi)*

Applicant presents the following issues for review: Whether the Office has established a prima facie case of obviousness in rejecting Claims 1, 4, 5, 9, 10, 14, 15, 16, 19, 20, 23, 24 and 28-34 under 35 U.S.C. § 103(a) as being unpatentable over Nakagawa in view of Wright and further in view of McMillan.

7. *ARGUMENT – UNDER 37 C.F.R. § 41.37(c)(1)(vii)*

Pursuant to 37 C.F.R. § 41.37(c)(1)(vii), the following provides the contentions of Applicant with respect to the grounds of rejection above in accordance with 37 C.F.R. § 41.37(c)(1)(vi). In accordance with 37 C.F.R. § 41.37(c)(1)(vii), claims argued separately and/or in a group are placed under an appropriate subheading to identify the claims by number.

Applicant respectfully submits that the references of record do not disclose any insurance products or methods that protect the privacy of the consumer while providing insurance premiums that are adjusted based on use of the vehicle. In one aspect of the invention: the privacy of the consumer can be protected because only cost information is transmitted from the computation device so privacy concerns surrounding real time location of the vehicle are protected because the computation device only transmits a dollar amount. *See Application at Pg. 12, Ln. 3-8 (emphasis added).*

Claims 1, 4, 5, 9, 10, 14 and 15

Applicant defines the invention in Claim 1 which recites, in part:

> deriving a first cost increment by evaluating at least the location information, the vehicle performance information and a pricing database,
> wherein the deriving of the first cost increment is performed on the vehicle;
> transmitting the first cost increment from the billing transmission system to the contracting company,
> wherein the first cost increment is devoid of the location information and the vehicle performance information.

Claim 16 recites, in part:

> a transmitting device that sends the first cost increment to the contracting company,
> wherein the first cost increment is devoid of the location information and the vehicle performance information,
> wherein access to the performance information and the location information of the vehicle is restricted by at least encrypting the location information and the vehicle performance information.

Claim 30 recites, in part:

> transmitting the first incremental insurance cost to the contracting company,
> wherein the first incremental insurance cost is devoid of the operational factor and restricting access by at least encrypting the operational factor.

Applicant respectfully submits to the Board that the Office has erred in not establishing a prima facie case of obviousness under 35 U.S.C. § 103. With specific reference to the limitations of the claims as set forth above, Applicant respectfully submits that the Office has set forth an insufficient record to establish the prima facie case under 35 U.S.C. § 103(a) because Nakagawa alone or in combination with McMillan and Wright does not teach or suggest every limitation as set forth in the claims and especially those underlined above. In addition to not teaching every limitation in the

claims, using the Office's interpretation of Nakagawa, Nakagawa would *teach away* from the combination of McMillan and Wright and, therefore, such a combination cannot support the alleged prima facie case under 35 U.S.C. § 103(a).

In an attempt to make it plain to the Board that the Office has not provided a sufficient record to support the obviousness rejection of Claim 1 under 35 U.S.C. § 103, Applicant sets forth below the record - in its entirety - that refers to above-discussed limitations of Claim 1.

> Application/Control Number: 10/674,929 Page 3
> Art Unit: 3626
>
> -transmitting said first cost increment from the billing transmission system to the contracting company, wherein said first cost increment is devoid of said location information and said vehicle performance information **(Nakagawa: para. 0032-0035; para. 0095-0096)**;
>
> -transmitting said second cost increment from the billing transmission system to the contracting company, wherein said second cost increment is devoid of location information and said vehicle performance information; and
>
> -preparing billing for the customer from the contracting company based on at least said first and said second cost increments.

Applicant submits that the office action lacks sufficient detail to support the rejection of the claim limitation that the first cost increment is devoid of the location information and the vehicle performance information, as recited in Claim 1. Moreover, the paragraphs in Nakagawa identified in the office action (i.e., para. [0032]-[0035], [0095] and [0096]) do not support the rejection of the Claims.

In support of the above, Applicant directs the Board's attention to paragraphs [0032] – [0035] which are the final four paragraphs of the thirty-one paragraphs that make up the Summary of the Invention in Nakagawa. Paragraphs [0032] – [0035] tell the public that the device in Nakagawa appears to detect:

how you drive your car,

how well you maintain your car and

whether you implement safety equipment.

See Nakagawa at Ln. 1-4 of para. [0032] and Ln. 1-4 of para. [0035].

Paragraphs [0095] and [0096] then succinctly inform the public that the device in Nakagawa takes all of this information from the onboard system and sends it to the car insurance company. *See Nakagawa at Ln. 7-11 of para [0095].*

Far from being devoid of such information that the consumer does not want to share, Nakagawa tells the public that any factor that adjusts the cost of the vehicle insurance is routinely shared and sent to the billing company.

In Nakagawa for example, the car insurance company 2 calculates the car insurance premiums based on information sent by radio communication from car 1 and information sent from the contract repair factory 3. When a user has properly installed safety equipment in car 1, drives car 1 safely, and properly maintains and manages car 1 at contract repair factory 3, car insurance company 2 assumes a reduction in any insurance that may have to be paid out for car 1. Therefore, the insurance premiums payable for car 1 are discounted. Conversely, if the user 1 has not properly installed safety equipment in car 1, does not drive safely, and does not properly maintain or

manage car 1, car insurance company 2 assumes an increase in any insurance that may have to be paid out for car 1. Therefore, the car insurance premiums payable for that car are increased. Data relating to the car insurance premiums after any discount or increase has been applied is sent via radio communication from car insurance company 2 to car 1. The received data relating to the car insurance premium is displayed so that it is visible to the user of car 1. *See Nakagawa at para [0050]*.

Even beyond safety measures and car information, the system in Nakagawa can use an air analyzer or breath tester to detect whether or not a user has consumed alcohol and the levels consumed. The operating status detection means 7 also includes various sensors for collecting information relating to the operating status of car 1. All of this is reported back to the billing company. *See Nakagawa at para [0054]*.

Applicant submits that the disclosure Nakagawa cannot support the rejection of Claim 1 that recites, in part: transmitting the first cost increment from the billing transmission system to the contracting company, wherein the first cost increment is devoid of the location information and the vehicle performance information.

Claims 16, 19, 20, 23, 24, 28 and 29

Applicant sets forth below the record - in its entirety - that refers to the above-discussed limitations of Claim 16.

-a computation device configured to acquire location information of the vehicle and derive a cost increment by evaluating at least said location information and a pricing database **(Nakagawa: para. 0053; para. 0061)**; and

-a transmitting device to send said cost increment to the contracting company, wherein said cost increment essentially consists of monetary information **(Nakagawa: para. 0053; i.e. on-board radio part)**.

Claims 16 amended with the same limitations as claim 1, therefore the rejection, remarks, and motivation for claim 1 applies to claim 16. Applicant should refer to claim 1 rejections' limitations to apply to claim 16.

First of all, the office action refers to "a transmitting device to send said cost increment to the contracting company, wherein said cost increment essentially consists of monetary information." The above quoted limitations of Claim 16 are actually from a previous version of Claim 16. *See Amendment having mail room date October 25, 2007 at Pg. 6 at Exhibit 6.* Applicant can only draw the conclusion that the Examiner has not read Claim 16 and is merely recycling old versions of previous office actions. Because the Office has failed to supply any reasons on the record for the current version of Claim 16, other than those set forth before Claim 1, Applicant submits that the Office action lacks sufficient detail to support the rejection of Claim 16 for at least the reasons set forth for Claim 1 above.

Applicant sets forth below the record – in its entirety – that refers to the above-discussed limitations of Claim 30.

> Application/Control Number: 10/674,929 Page 9
> Art Unit: 3626
>
> Claims 30 amended with the same limitations as claim 1, therefore the rejection, remarks, and motivation for claim 1 applies to claim 30. Applicant should refer to claim 1 rejection's limitations to apply to claim 30.

As noted above in the office action with reference to Claim 30, the office action offers nothing new with regard to Claim 30 and asks the Applicant to refer back to Claim 1. As such, Applicant submits Claim 30 and its dependent claims are allowable for the same reasons as set forth for Claim 1.

Applicant respectfully submits that neither the paragraphs in Nakagawa identified in the portions of the office action (reproduced above) nor anything disclosed in Nakagawa, Wright, McMillan or any of the references of record support the rejection under 35 U.S.C. § 103(a).

It needs to be noted that the office action only cites Nakagawa when rejecting the claim limitation that the first cost increment is devoid of the location information and the vehicle performance information, as recited in Claims 1 and 30. Even though the office action does not rely on Wright or McMillan, Wright and McMillan only provide for the gathering of various pieces of vehicle parameters and information. All of these various pieces of vehicle parameters and information are sent back to the billing company. *See, e.g., Wright at Col. 3, Ln. 7-19 and McMillan at Col. 6, Ln. 58-62.*

If we follow the logic of the office action, Nakagawa allegedly discloses that what is transmitted to the insurance company does not include location information or vehicle information. While Applicant does not acquiesce to this interpretation, if we assume Nakagawa does as such, there can be no proper combination with Wright and McMillan because Nakagawa, the primary reference, *teaches away* from Wright and McMillan. This is so because Wright and McMillan disclose that all the various pieces of vehicle parameters and information are sent back to the billing company. *See, e.g., Wright at Col. 3, Ln. 7-19 and McMillan at Col. 6, Ln. 58-62.* When the Office interprets Nakagawa to be so protective of privacy, the Office cannot then claim the combination with Wright and McMillan is obvious when Wright and McMillan do what is contrary to the alleged protections of Nakagawa. Because Nakagawa *teaches away* from the combination with Wright and McMillan, the Office can only produce such a combination with impermissible hindsight based on the teachings in the present application.

8. CLAIMS APPENDIX – UNDER 37 C.F.R. § 41.37(c)(1)(viii)

A copy of the claims involved in this Appeal, namely claims 1, 4, 5, 9, 10, 14, 15, 16, 19, 20, 23, 24, and 28-34 is attached as a claims appendix.

9. EVIDENCE APPENDIX – UNDER 37 C.F.R. § 41.37 (c)(1)(ix)

The following items listed below are attached as an evidence appendix.

A. A copy of the claims presently being appealed (i.e., Claims 1, 4, 5, 9, 10, 14, 15, 16, 19, 20, 23, 24 and 28-34) is provided in the attached Claims Appendix in accordance with 37 C.F.R. § 41.37 (c)(1)(viii).

B. A copy of the Office Action mailed January 30, 2008, placing the present application under final rejection is provided in the attached Evidence Appendix as Exhibit 1 in accordance with 37 C.F.R. § 41.37 (c)(1)(ix).

C. A copy of United States Patent Publication Number 2002/0128882 to Nakagawa et al. (hereinafter Nakagawa) is provided in the attached Evidence Appendix as Exhibit 2 in accordance with 37 C.F.R. § 41.37(c)(1)(ix).

D. A copy of United States Patent Number 6,052,466 to Wright is provided in the attached Evidence Appendix as Exhibit 3 in accordance with 37 C.F.R. § 41.37(c)(1)(ix).

E. A copy of United States Patent Number 5,797,134 to McMillan et al. (hereinafter McMillan) is provided in the attached Evidence Appendix as Exhibit 4 in accordance with 37 C.F.R. § 41.37(c)(1)(ix).

F. A copy of the Application imaged with line numbers is provided in the attached Evidence Appendix as Exhibit 5 in accordance with 37 C.F.R. § 41.37(c)(1)(ix) and is provided to facilitate citation to the Application pursuant to 37 C.F.R. § 41.37(c)(1)(v) in the applicable sections below.

G. A copy of the Amendment having mail room date October 25, 2007, is provided in the attached evidence Appendix as Exhibit 6 in accordance with 37 C.F.R. § 41.37(c)(1)(ix).

10. RELATED PROCEEDINGS APPENDIX – UNDER 37 C.F.R. § 41.37 (c)(1)(x)

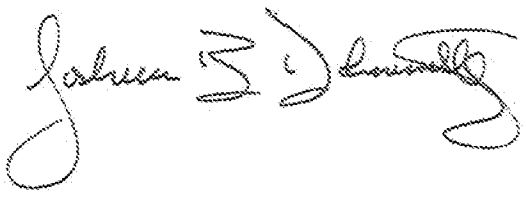
None.

CONCLUSION

Applicant respectfully submits that the Office has not established a prima facie case of obviousness in the rejection of Claims 1, 4, 5, 9, 10, 14, 15, 16, 19, 20, 23, 24 and 28-34. Accordingly, reversal of the above rejections and removal of the finality of the office action are respectfully requested. Applicant believes that Claims 1, 4, 5, 9, 10, 14, 15, 16, 19, 20, 23, 24 and 28-34 are in condition for allowance. As always, the Office is invited to contact the undersigned at (248) 641-1600 to facilitate prosecution of this application.

Respectfully submitted,

Date: October 23, 2008



Joshua B. Dobrowitsky, Reg. No. 51,288
Mark D. Elchuk, Reg. No. 33,686

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield, Michigan 48303
(248) 641-1600

[MDE/JBD/tdh]

Claims Appendix
Under 37 C.F.R. § 41.37(c)(1)(viii)

LISTING OF CLAIMS

1. A method of calculating automobile insurance for a vehicle of a customer of a contracting company, the method comprising:

acquiring location information of the vehicle with a location system on the vehicle;

acquiring vehicle performance information from the vehicle;

deriving a first cost increment by evaluating at least said location information, said vehicle performance information and a pricing database, wherein said deriving of said first cost increment is performed on the vehicle;

connecting a billing transmission system on the vehicle with the contracting company;

transmitting said first cost increment from the billing transmission system to the contracting company, wherein said first cost increment is devoid of said location information and said vehicle performance information;

restricting access to by at least encrypting said location information and said vehicle performance information;

accessing by at least decrypting said location information and said vehicle performance information with an access key, wherein said access key consists of a first passkey retained by the customer and a second passkey retained by the contracting company;

providing access for the customer outside of the vehicle to said first cost increment prior to the contracting company billing the customer, wherein said

providing access to said first cost increment is adapted to permit the customer to alter driving habits to adjust a second cost increment;

transmitting said second cost increment from the billing transmission system to the contracting company, wherein said second cost increment is devoid of said location information and said vehicle performance information; and

preparing billing for the customer from the contracting company based on at least said first and said second cost increments.

2. (CANCELED)

3. (CANCELED)

4. The method of calculating automobile insurance of Claim 1, wherein said location information includes at least one of a geographical location of the vehicle, a duration of time the vehicle is located at said geographical location, a vehicle speed, an applicable speed limit, and combinations thereof.

5. The method of calculating automobile insurance of Claim 1, wherein said vehicle performance information includes at least one of a vehicle speed, a vehicle acceleration rate, a vehicle deceleration rate, a vehicle maintenance status, an engine speed, a brake force, a vehicle payload, and combination thereof.

6. – 8. (CANCELED)

9. The method of calculating automobile insurance of Claim 1, wherein said location system includes at least one of a global positioning satellite receiver to determine location and a geographical database configured to be resident on the device.

10. The method of calculating automobile insurance of Claim 1, wherein said pricing database at least includes actuarial statistics.

11 – 13. (CANCELED)

14. The method of calculating automobile insurance of Claim 1, wherein said providing access for the customer to said first cost increment includes at least one of internet web site interface, a phone interface, a customer service interface, and combinations thereof.

15. The method of calculating automobile insurance of Claim 1, wherein transmitting said first cost increment includes at least one of establishing a cellular phone connection, establishing a radio connection, establishing microwave communication, establishing a phone connection, establishing an internet connection, and combinations thereof.

16. A vehicle insurance computation apparatus that is installed in a vehicle and communicates with a contracting company that is remote to the vehicle and provides billing to a customer, the vehicle insurance computation apparatus comprising:

a computation device that acquires location information of the vehicle, acquires vehicle performance information from the vehicle and derives a first cost increment by evaluating at least said location information, said performance information and a pricing database; and

a transmitting device that sends said first cost increment to the contracting company, wherein said first cost increment is devoid of said location information and said vehicle performance information,

wherein access to said performance information and said location information of the vehicle is restricted by at least encrypting said location information and said vehicle performance information,

wherein access is granted by at least decrypting said location information and said vehicle performance information with an access key,

wherein said access key consists of a first passkey retained by the customer and a second passkey retained by the contracting company,

wherein said computation device is configured to provide access for the customer outside of the vehicle to said first cost increment prior to the billing of the customer by contracting company,

wherein said access for the customer outside of the vehicle to said first cost increment is adapted to permit the customer to alter driving habits to adjust a second cost increment;

wherein said transmitting device sends said second cost increment to the contracting company,

wherein said second cost increment is devoid of said location information and said vehicle performance information, and

wherein said sending of said second cost increment to the contracting company permits the contracting company to prepare the billing for the customer based on at least said first and said second cost increments.

17. (CANCELED)

18. (CANCELED)

19. The apparatus of Claim 16, wherein said location information of the vehicle includes at least one of a geographical location of the vehicle, a duration of time the vehicle is located at said geographical location, a vehicle speed, an applicable speed limit, and combinations thereof.

20. The apparatus of Claim 16, wherein said performance information of the vehicle includes at least one of a vehicle speed, a vehicle acceleration rate, a vehicle deceleration rate, a vehicle maintenance status, an engine speed, a brake force, a vehicle payload, and combinations thereof.

21. (CANCELED)

22. (CANCELED)

23. The apparatus of Claim 16, wherein said computation device includes at least one of a global positioning satellite receiver to determine location and a geographical database configured to be resident on the device.

24. The apparatus of Claim 23, wherein said pricing database at least includes actuarial statistics.

25. (CANCELED)

26. (CANCELED)

27. (CANCELED)

28. The apparatus of Claim 16, wherein said computation device is configured to provide access for the customer outside of the vehicle through at least one of an internet web site interface, a phone interface, a customer service interface, and combinations thereof.

29. The apparatus of Claim 16, wherein said transmitting device includes at least one of a cellular phone connection, a radio connection, microwave communication, a phone connection, an internet connection, and combinations thereof.

30. A method of determining a cost of insuring a motor vehicle, comprising:

using a monitoring apparatus located on-board the motor vehicle to at least assist in monitoring an operational factor associated with the motor vehicle in real time;

recording information relating to said operational factor;

determining a first incremental insurance cost with said recorded information for the motor vehicle related to a given incremental time period;

transmitting said first incremental insurance cost to the contracting company, wherein said first incremental insurance cost is devoid of said operational factor;

restricting access to by at least encrypting said operational factor;

accessing by at least decrypting said operational factor with an access key, wherein said access key consists of a first passkey retained by the customer and a second passkey retained by the contracting company;

providing access for the customer outside of the motor vehicle to said first incremental insurance cost prior to the contracting company billing the customer, wherein said providing access to said first incremental insurance cost is adapted to permit the customer to alter driving habits to adjust a second incremental insurance cost;

transmitting said second incremental insurance cost to the contracting company, wherein said second incremental insurance cost is devoid of said operational factor; and

preparing billing for the customer from the contracting company based on at least said first and said second incremental insurance costs.

31. The method of claim 30, further comprising having an underwriting entity provide the operator with a charge for an insuring the motor vehicle, based on said first and said second incremental insurance costs, for said given incremental time period.

32. The method of claim 30, wherein determining said first incremental insurance cost comprises using a cost calculation system and a cost lookup database on the motor vehicle having actuarial information, in addition to said operational factor.

33. The method of claim 30, wherein monitoring said operational factor of the motor vehicle comprises monitoring at least one of the group of variable comprising:

a speed of the motor vehicle;

a geographic location of the motor vehicle;

an acceleration of the motor vehicle; and

a deceleration of the motor vehicle.

34. The method of claim 33, further comprising using an external location identification system for assisting in determining said geographic location of the motor vehicle.

Evidence Appendix
Under 37 C.F.R. § 41.37(c)(1)(ix)

Exhibit 1

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/674,929	09/30/2003	Rodney B. Kendrick	7784-000652	5150

65961 7590 01/30/2008

HARNESS DICKEY & PIERCE, PLC
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
RANGREJ, SHEETAL	

ART UNIT	PAPER NUMBER
3626	

MAIL DATE	DELIVERY MODE
01/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/674,929	KENDRICK, RODNEY B.	
	Examiner	Art Unit	
	SHEETAL R. RANGREJ	3626	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 October 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4,5,9,10,14-16,19,20,23,24 and 28-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 4, 5, 9, 10, 14-16, 19, 20, 23, 24, and 28-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Prosecution History Summary

1. Claims 1, 4, 5, 9, 10, 14-16, 19, 20, 23, 24, and 28-34 are pending.

2. Claims 1, 4, 5, 14, 15, 16, 20, 23, 24, and 28-34 are amended.

3. Claims 2, 3, 6, 7, 8, 12, 13, 17, 18, 21, 22, and 25-27 are cancelled.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 4, 5, 9, 10, 14-16, 19, 20, 23, 24, and 28-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakagawa et al. (U.S. Publication No. 2002/0128882) in view of Wright (U.S. Patent No. 6,052,466) and further in view of McMillan et al. (U.S. Patent No. 5,797,134).

6. As per claim 1, Nakagawa teaches a method of calculating automobile insurance for a vehicle of a customer of a contracting company, the method comprising:

-acquiring location information of the vehicle with a location system on the vehicle **(Nakagawa: para. 0053-0054)**;

-deriving a first cost increment by evaluating at least said location information, said vehicle performance information and a pricing database, wherein said deriving of said first cost increment is performed on the vehicle **(Nakagawa: para. 0053-0057)**;

-connecting a billing transmission system on the vehicle with the contracting company **(Nakagawa: para. 0059)**

-transmitting said first cost increment from the billing transmission system to the contracting company, wherein said first cost increment is devoid of said location information and said vehicle performance information **(Nakagawa: para. 0032-0035; para. 0095-0096)**;

-transmitting said second cost increment from the billing transmission system to the contracting company, wherein said second cost increment is devoid of location information and said vehicle performance information; and

-preparing billing for the customer from the contracting company based on at least said first and said second cost increments.

Generating different amounts (i.e. first and second cost increments) does not change the invention as a whole and goes through the same process at deriving the costs and therefore Nakagawa's system teaches generation of cost increments as stated.

Nakagawa does not teach a method of calculating automobile insurance for a vehicle of a customer of a contracting company, the method comprising: -restricting access to by at least encrypting said information and said vehicle performance information, -accessing by at least decrypting said location information and said vehicle performance information with an access key, wherein said access key consists of a first passkey retained by the customer and a second passkey retained by a contracting company, and -providing access for the customer outside of the vehicle to said first cost increment prior to the contracting company billing the customer, wherein said providing access to said first cost increment is adapted to permit the customer to alter driving habits to adjust a second cost increment.

Wright teaches a method of calculating automobile insurance for a vehicle of a customer of a contracting company, the method comprising: restricting access to by at least encrypting

said information and said vehicle performance information **(Wright: col. 5, 19 to col.. 6, 2)** and accessing by at least decrypting said location information and said vehicle performance information with an access key, wherein said access key consists of a first passkey retained by the customer and a second passkey retained by a contracting company **(Wright: col. 5, 19 to col.. 6, 2)**.

One of ordinary skill in the art at the time the invention was made would have found it obvious to combine the teachings of Nakagawa and Wright with the motivation that if communication concerns sensitive information that it is common for the parties to employ a security protocol (such as encryption) to prevent the eavesdropper from being able to discover the communicated information **(Wright: col. 1, 14-23)**.

Wright does not teach a method of calculating automobile insurance for a vehicle of a customer of a contracting company, the method comprising providing access for the customer outside of the vehicle to said first cost increment prior to the contracting company billing the customer, wherein said providing access to said first cost increment is adapted to permit the customer to alter driving habits to adjust a second cost increment.

McMillan teaches a method of calculating automobile insurance for a vehicle of a customer of a contracting company, the method comprising providing access for the customer outside of the vehicle to said first cost increment prior to the contracting company billing the customer, wherein said providing access to said first cost increment is adapted to permit the customer to alter driving habits to adjust a second cost increment **(McMillan: col. 6, 23-29)**.

One of ordinary skill in the art at the time the invention was made would have found it obvious to combine the teachings of Nakagawa in view of Wright and McMillan with the

motivation that none of the data obtained through conventional systems reliably predict the manner or safety of future operation of the vehicle and to help drivers make better decisions about driving habits **(McMillan: col. 2, 40-55)**.

7. As per claim 4, the method of claim 1 is as described. Nakagawa and Wright do not teach wherein said location information includes at least one of a geographical location of the vehicle, a duration of time the vehicle is located at said geographical location, a vehicle speed.

McMillan teaches wherein said location information includes at least one of a geographical location of the vehicle **(McMillan: col. 6, 58-62)**, a duration of time the vehicle is located at said geographical location **(McMillan: col. 4, 35-36)**, a vehicle speed **(McMillan: col. 7, 60)**.

The motivation to combine the teachings is the same as claim 1.

8. As per claim 5, the method of claim 1 is as described. Nakagawa and Wright do not teach wherein said vehicle information includes at least one of a vehicle speed.

McMillan teaches wherein said vehicle information includes at least one of a vehicle speed **(McMillan: col. 7, 60)**.

The motivation to combine the teachings is the same as claim 1.

9. As per claim 9, the method of claim 1 is as described. Nakagawa and Wright do not teach wherein said location system includes at least one of a global positioning satellite receiver to determine location and a geographical database configured to be resident on the device.

McMillan teaches wherein said location system includes at least one of a global positioning satellite receiver to determine location and a geographical database configured to be resident on the device **(McMillan: col. 6, 58-62)**.

The motivation to combine the teachings is the same as claim 1.

10. As per claim 10, the method of claim 1 is as described. Nakagawa and Wright do not teach wherein said pricing database at least includes actuarial statistics.

McMillan teaches wherein said pricing database at least includes actuarial statistics **(McMillan: col. 4, 28-59)**.

The motivation to combine the teachings is the same as claim 1.

11. As per claim 14, the method of claim 1is as described. Nakagawa further teaches wherein said providing access for the customer to said first cost increment includes at least one of internet web site interface, a phone interface, a customer service interface, and combinations thereof **(Nakagawa: para. 0053; para. 0057)**. The examiner interprets that the display means is the same as any interface receiving data from a remote location.

12. As per claim 15, the method of claim 1 is as described. Nakagawa and Wright do not teach wherein transmitting said cost increment includes at least one of establishing a cellular phone connection, establishing a radio connection, establishing microwave communication, establishing a phone connection, establishing an internet connection, and combinations thereof.

McMillan teaches wherein transmitting said cost increment includes at least one of establishing a cellular phone connection, establishing a radio connection, establishing microwave communication, establishing a phone connection, establishing an internet connection, and combinations thereof **(McMillan: col. 6, 62-64)**.

The motivation to combine the teachings is the same as claim 1.

13. As per claim 16, Nakagawa teaches a vehicle insurance computation device that is installed in a vehicle and communicates with a contracting company comprising:

-a computation device configured to acquire location information of the vehicle and derive a cost increment by evaluating at least said location information and a pricing database **(Nakagawa: para. 0053; para. 0061)**; and

-a transmitting device to send said cost increment to the contracting company, wherein said cost increment essentially consists of monetary information **(Nakagawa: para. 0053; i.e. on-board radio part)**.

Claims 16 amended with the same limitations as claim 1, therefore the rejection, remarks, and motivation for claim 1 applies to claim 16. Applicant should refer to claim 1 rejections' limitations to apply to claim 16.

14. As per claims 19-20: As the underlying process has been shown to be fully disclosed by the teachings of Nakagawa in view of Wright and further in view of McMillan in the above rejection of claims 4-5, it is readily apparent that the Nakagawa in view of Wright and further in view of McMillan references includes a system to perform the recited functions. As such, these limitations are rejected for the same reasons provided in the rejection of claims 4-5 and incorporated herein.

15. As per claims 23-24: As the underlying process has been shown to be fully disclosed by the teachings of Nakagawa in view of Wright and further in view of McMillan in the above rejection of claims 9-10, it is readily apparent that the Nakagawa in view of Wright and further in view of McMillan references includes a system to perform the recited functions. As such, these limitations are rejected for the same reasons provided in the rejection of claims 9-10 and incorporated herein.

16. As per claim 28: As the underlying process has been shown to be fully disclosed by the teachings of Nakagawa in view of Wright and further in view of McMillan in the above rejection of claims 14, it is readily apparent that the Nakagawa in view of Wright and further in view of McMillan references includes a system to perform the recited functions. As such, these limitations are rejected for the same reasons provided in the rejection of claims 14 and incorporated herein.

17. As per claim 29: As the underlying process has been shown to be fully disclosed by the teachings of Nakagawa in view of Wright and further in view of McMillan in the above rejection of claim 15, it is readily apparent that the Nakagawa in view of Wright and further in view of McMillan references includes a system to perform the recited functions. As such, these limitations are rejected for the same reasons provided in the rejection of claim 15 and incorporated herein.

18. As per claim 30, Nakagawa teaches a method of determining a cost of insuring a motor vehicle, comprising:

-using a monitoring apparatus located on-board the motor vehicle to at least assist in monitoring an operational factor associated with the vehicle in real time **(Nakagawa: para. 0053; para. 0071)**;

-recording information relating to said operational factor **(Nakagawa: 0071)**; and

-using said recorded information to determine an incremental insurance cost for said motor vehicle related to a given incremental time period **(Nakagawa: para. 0073)**.

Claims 30 amended with the same limitations as claim 1, therefore the rejection, remarks, and motivation for claim 1 applies to claim 30. Applicant should refer to claim 1 rejection's limitations to apply to claim 30.

19. As per claim 31, the method of claim 30 is as described. Nakagawa further teaches further comprising having an underwriting entity provide the operator with a charge for an insuring the motor vehicle, based on said first and said second incremental insurance costs, for said given incremental time period **(Nakagawa: para. 0050)**.

20. As per claim 32, the method of claim 30 is as described. Nakagawa and Wright do not teach determining said first incremental insurance cost comprises using a cost calculation system and a cost lookup database on the motor vehicle having actuarial information, in addition to said operational factor.

McMillan teaches determining said first incremental insurance cost comprises using a cost calculation system and a cost lookup database on the motor vehicle having actuarial information, in addition to said operational factor **(McMillan: col. 4, 28-59)**.

The motivation to combine the teachings is the same as claim 1.

21. As per claim 33, the method of claim 30 is as described. Nakagawa further teaches wherein monitoring said operational factor of the motor vehicle comprises monitoring at least one of the group of variable comprising:

-a speed of the motor vehicle **(Nakagawa: para. 0072)**;

-an acceleration of the motor vehicle **(Nakagawa: para. 0072)**; and

-a deceleration of the motor vehicle **(Nakagawa: para. 0072)**.

22. As per claim 34, the method of claim 33 is as described. Nakagawa and Wright do not teach further comprising using an external location identification system for assisting in determining a geographic location of the motor vehicle.

McMillan teaches further comprising using an external location identification system for assisting in determining a geographic location of the motor vehicle **(McMillan: col. 6, 58-62)**.

The motivation to combine the teachings is the same as claim 2.

Response to Arguments

23. Applicant's arguments with respect to claims 1, 4, 5, 9, 10, 14-16, 19, 20, 23, 24, and 28-34 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

24. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHEETAL R. RANGREJ whose telephone number is (571)270-1368. The examiner can normally be reached on M-F 8:30-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas can be reached on 571-272-6776. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SRR SRR 1/18/08

C. LUKE GILLIGAN
PRIMARY EXAMINER
TECHNOLOGY CENTER 3600

Exhibit 2

US 20020128882A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2002/0128882 A1

Nakagawa et al. (43) Pub. Date: Sep. 12, 2002

(54) VEHICLE INSURANCE PREMIUM CALCULATION SYSTEM, ON-BOARD APPARATUS, AND SERVER APPARATUS

(75) Inventors: **Shigeru Nakagawa**, Okazaki-shi (JP); **Kenji Mori**, Toyota-shi (JP); **Akira Shinada**, Meguro-ku (JP); **Katsuhiko Nunokawa**, Kamakura-shi (JP); **Hiroaki Okajima**, Chiba-shi (JP); **Makoto Sasaki**, Chiba-shi (JP)

Correspondence Address:
OLIFF & BERRIDGE, PLC
P.O. BOX 19928
ALEXANDRIA, VA 22320 (US)

(73) Assignee: **TOYOTA JIDOSHA KABUSHIKI KAISHA**, Toyota-shi (JP)

(21) Appl. No.: **10/083,566**

(22) Filed: **Feb. 27, 2002**

(30) **Foreign Application Priority Data**

Mar. 6, 2001 (JP) 2001-062117

Publication Classification

(51) **Int. Cl.**[7] **G06F 17/60**

(52) **U.S. Cl.** **705/4**

(57) **ABSTRACT**

This system comprises a usage status detection means for detecting the usage status of a vehicle, data input means for inputting data relating to the maintenance or management of a vehicle, and insurance premium calculation means for calculating vehicle insurance premiums based on detection results and inputted data.

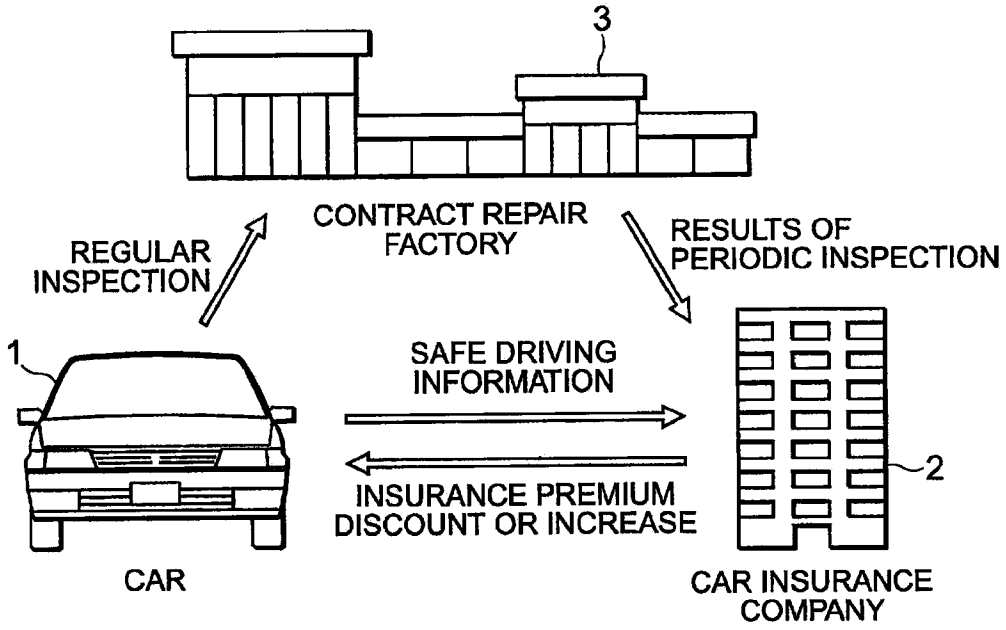
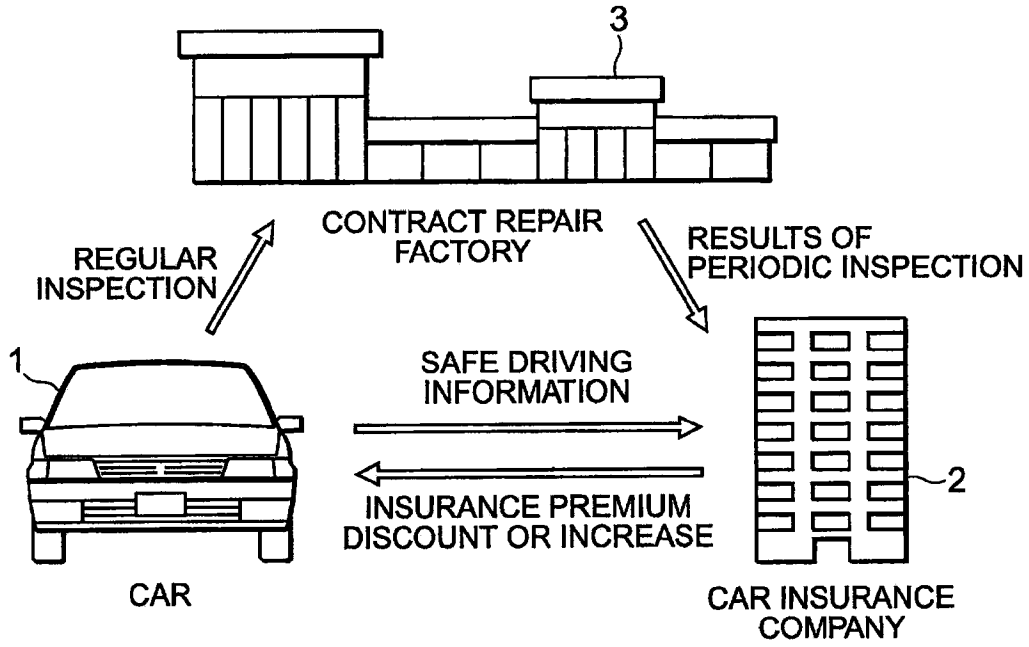


Fig.1


3
CONTRACT REPAIR FACTORY
REGULAR INSPECTION
RESULTS OF PERIODIC INSPECTION
1
SAFE DRIVING INFORMATION
INSURANCE PREMIUM DISCOUNT OR INCREASE
2
CAR
CAR INSURANCE COMPANY

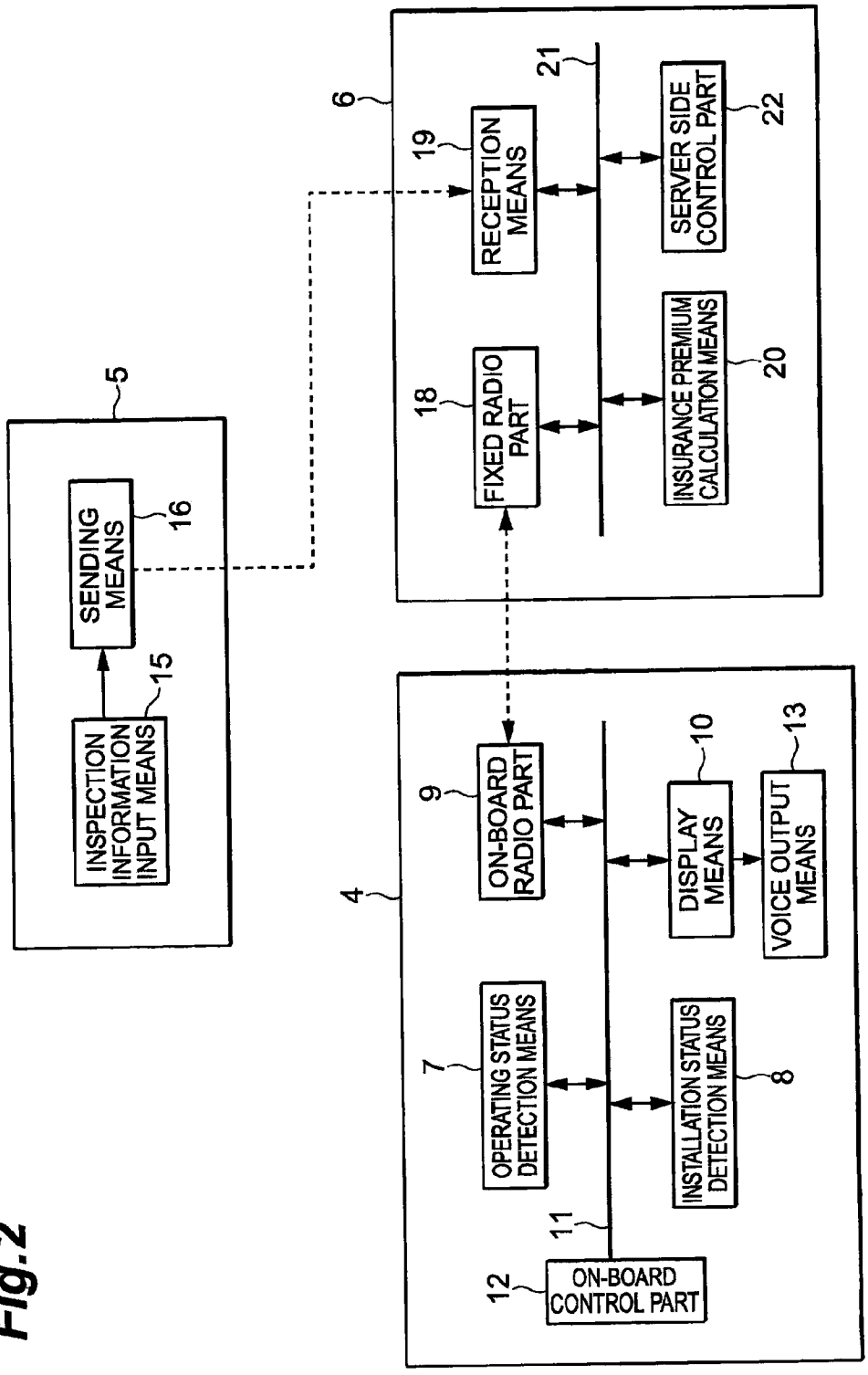

6
19
RECEPTION MEANS
21
SERVER SIDE CONTROL PART
22
18
FIXED RADIO PART
INSURANCE PREMIUM CALCULATION MEANS
20
5
SENDING MEANS
16
15
INSPECTION INFORMATION INPUT MEANS
4
9
ON-BOARD RADIO PART
10
DISPLAY MEANS
13
VOICE OUTPUT MEANS
7
OPERATING STATUS DETECTION MEANS
INSTALLATION STATUS DETECTION MEANS
8
11
12
ON-BOARD CONTROL PART

Fig.2

Fig.3

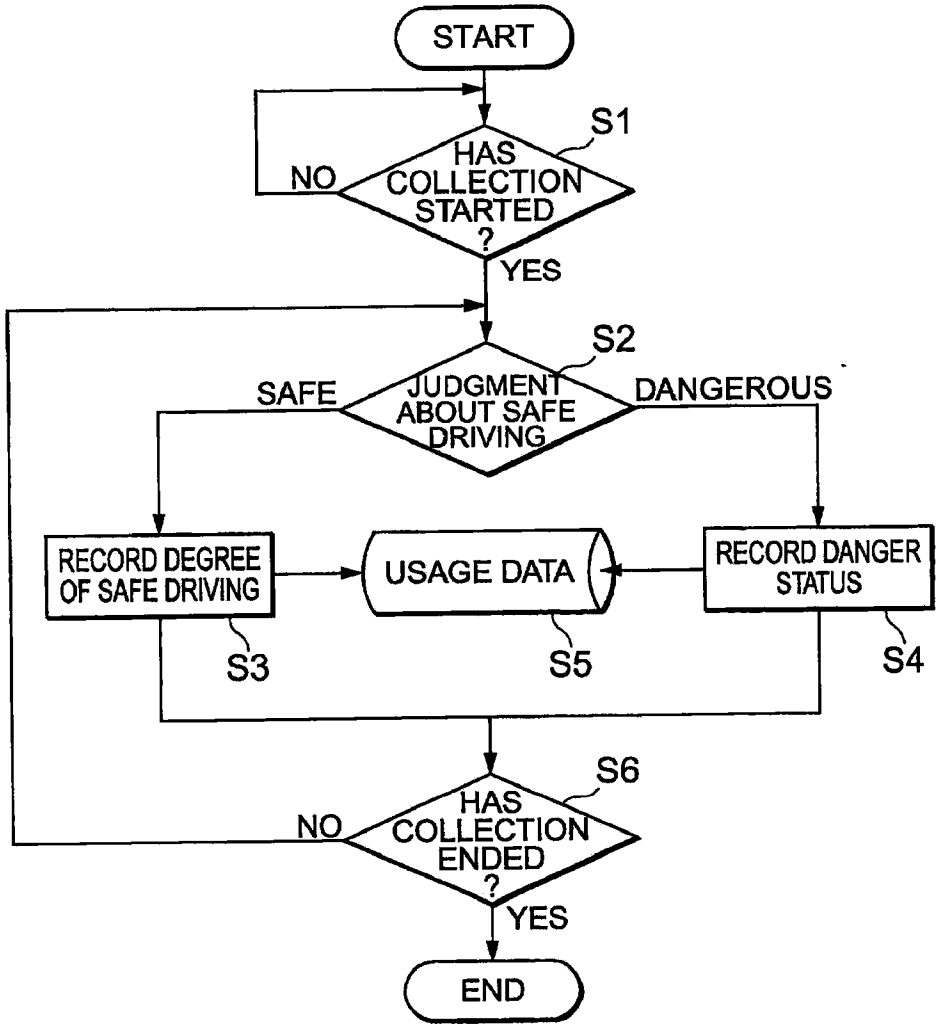

START
S1
HAS COLLECTION STARTED ?
NO
YES
S2
JUDGMENT ABOUT SAFE DRIVING
SAFE
DANGEROUS
RECORD DEGREE OF SAFE DRIVING
USAGE DATA
RECORD DANGER STATUS
S3
S5
S4
S6
HAS COLLECTION ENDED ?
NO
YES
END

Fig.4

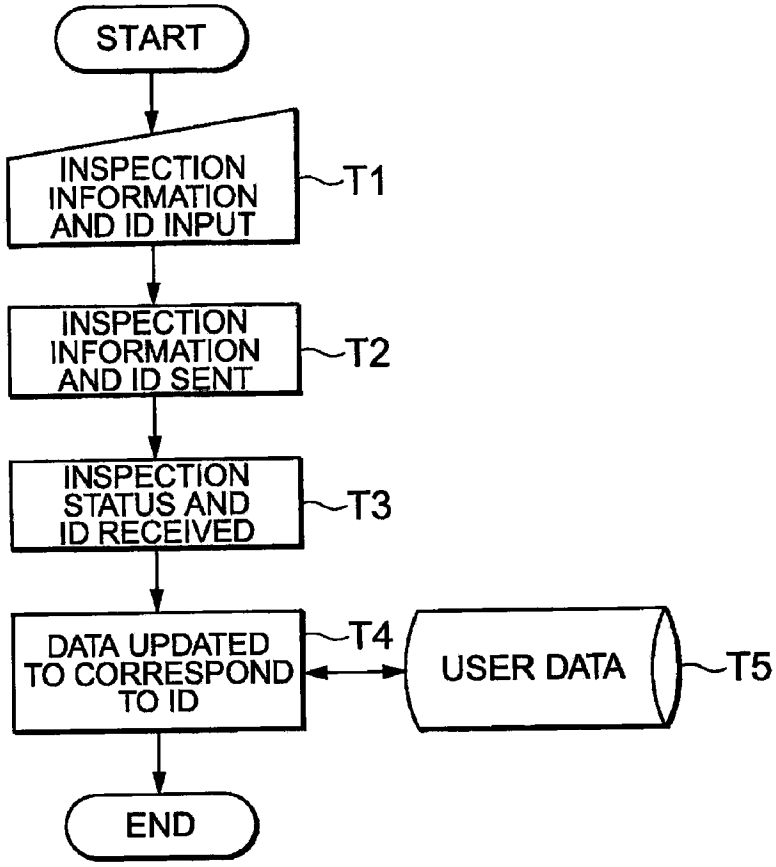

START
INSPECTION INFORMATION AND ID INPUT
T1
INSPECTION INFORMATION AND ID SENT
T2
INSPECTION STATUS AND ID RECEIVED
T3
DATA UPDATED TO CORRESPOND TO ID
T4
USER DATA
T5
END

Fig.5

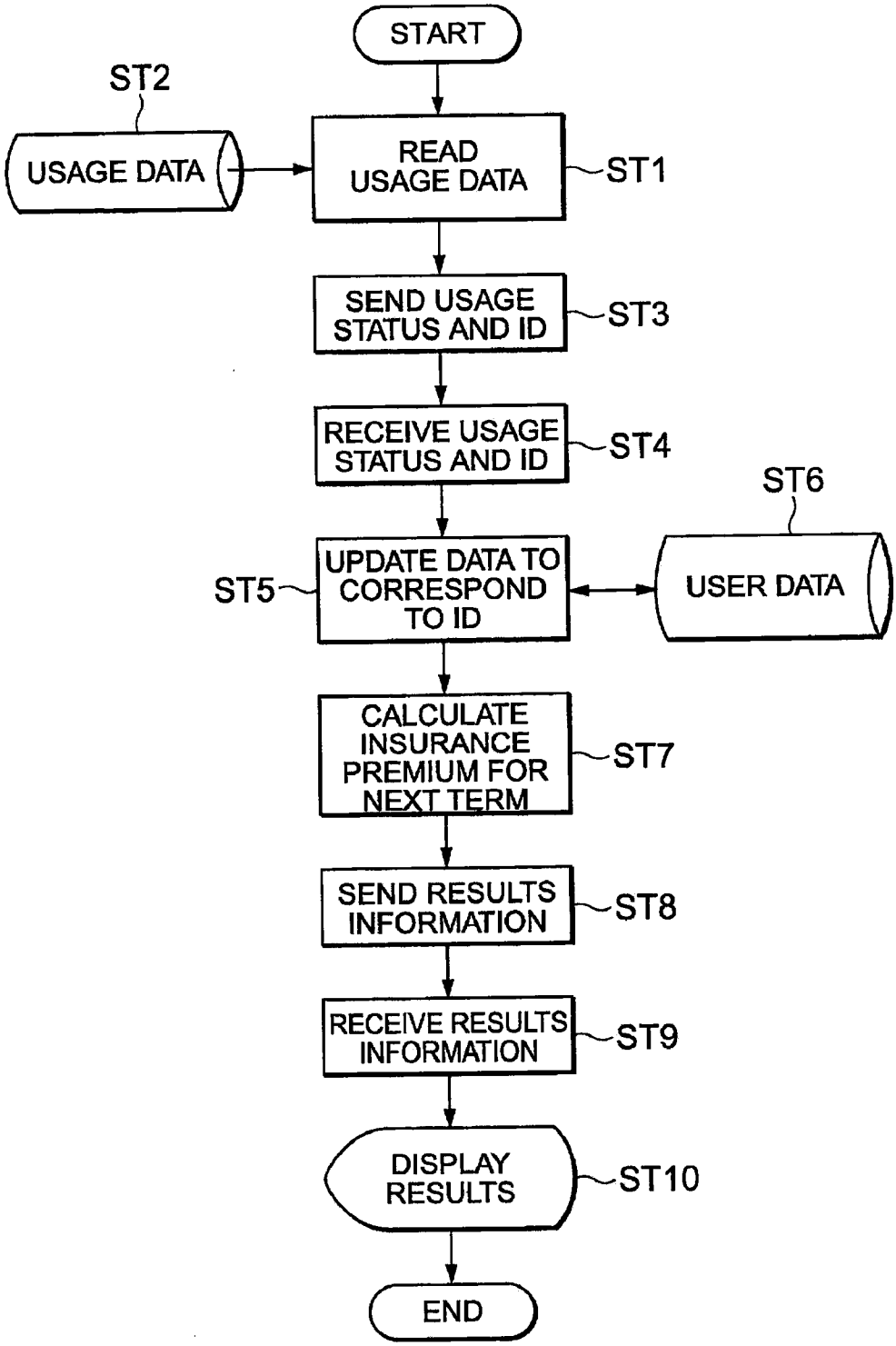
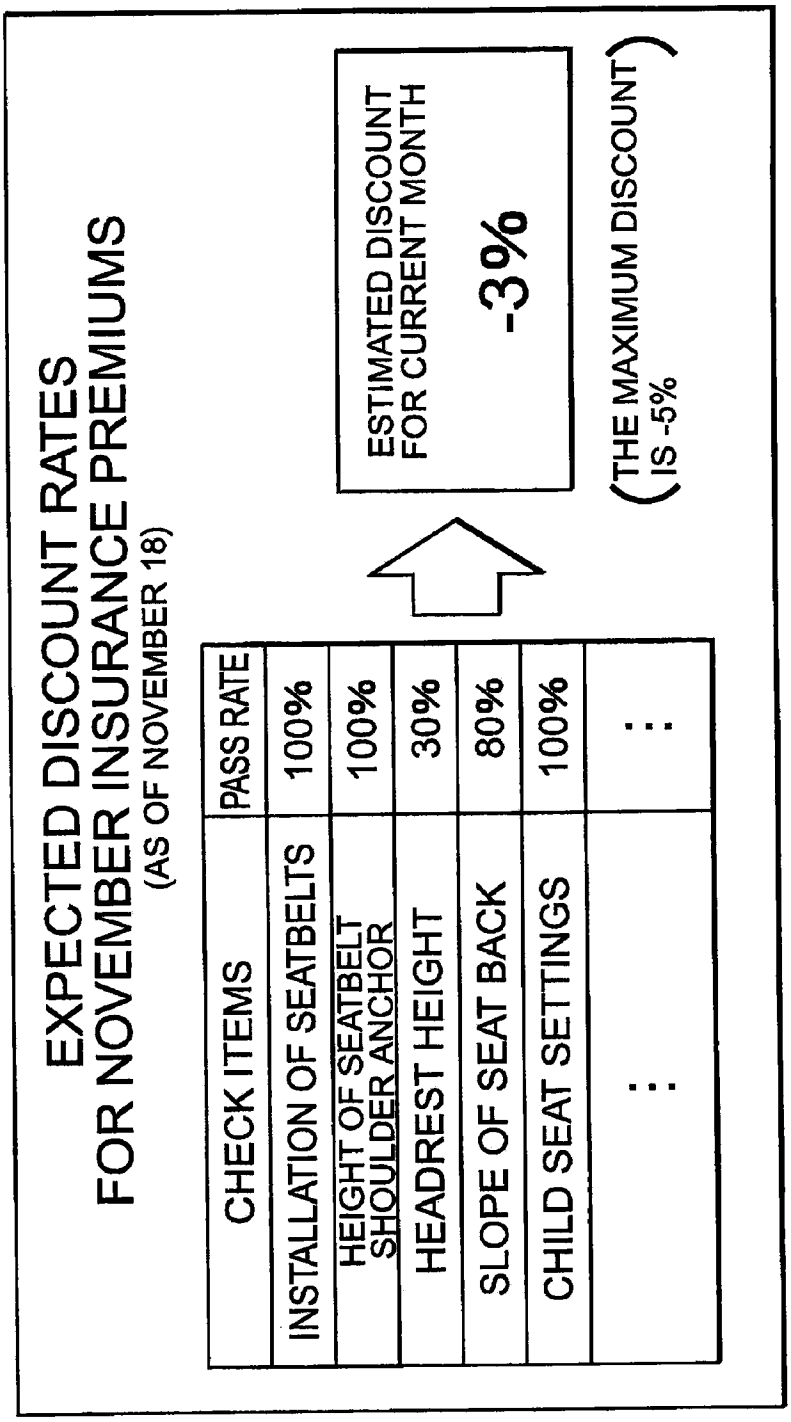

START
ST2
USAGE DATA
READ USAGE DATA
ST1
SEND USAGE STATUS AND ID
ST3
RECEIVE USAGE STATUS AND ID
ST4
ST6
ST5
UPDATE DATA TO CORRESPOND TO ID
USER DATA
CALCULATE INSURANCE PREMIUM FOR NEXT TERM
ST7
SEND RESULTS INFORMATION
ST8
RECEIVE RESULTS INFORMATION
ST9
DISPLAY RESULTS
ST10
END

Fig.6


EXPECTED DISCOUNT RATES
FOR NOVEMBER INSURANCE PREMIUMS
(AS OF NOVEMBER 18)
CHECK ITEMS
PASS RATE
INSTALLATION OF SEATBELTS
100%
HEIGHT OF SEATBELT SHOULDER ANCHOR
100%
HEADREST HEIGHT
30%
SLOPE OF SEAT BACK
80%
CHILD SEAT SETTINGS
100%
ESTIMATED DISCOUNT FOR CURRENT MONTH
-3%
(THE MAXIMUM DISCOUNT IS -5%)

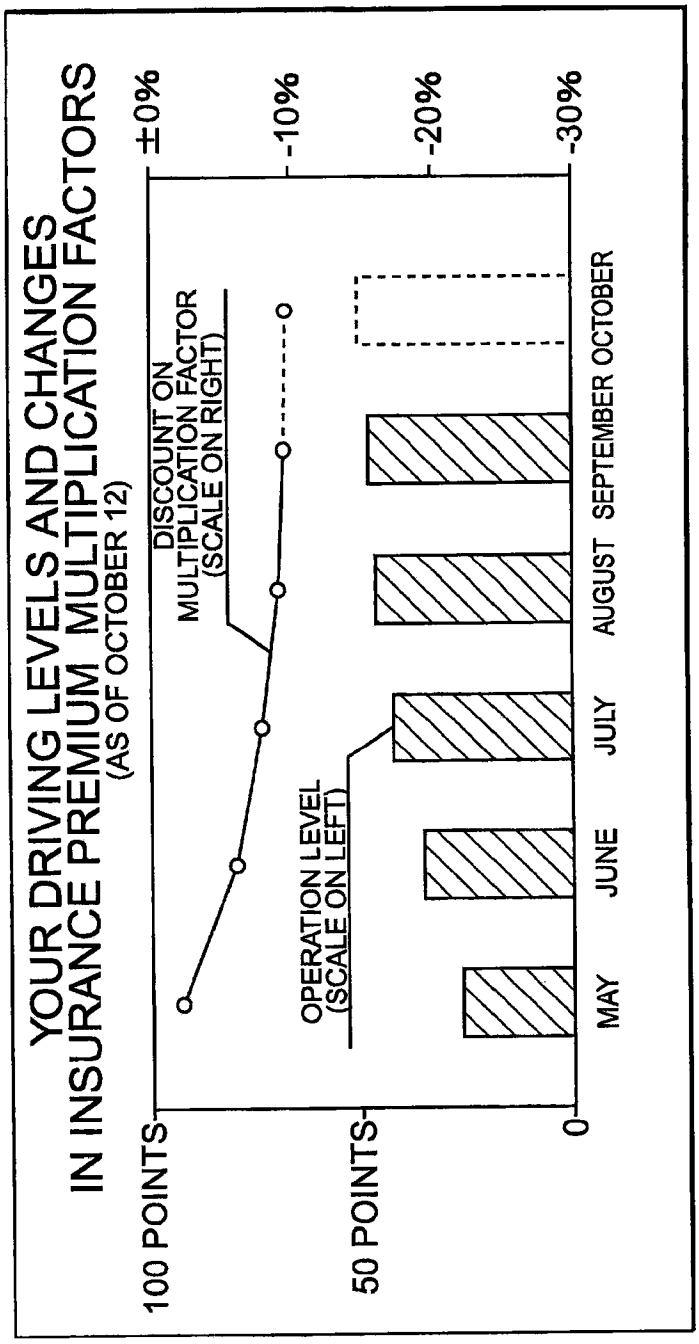

YOUR DRIVING LEVELS AND CHANGES
IN INSURANCE PREMIUM MULTIPLICATION FACTORS
(AS OF OCTOBER 12)
100 POINTS
50 POINTS
0
±0%
-10%
-20%
-30%
DISCOUNT ON
MULTIPLICATION FACTOR
(SCALE ON RIGHT)
OPERATION LEVEL
(SCALE ON LEFT)
MAY
JUNE
JULY
AUGUST
SEPTEMBER
OCTOBER

Fig.7

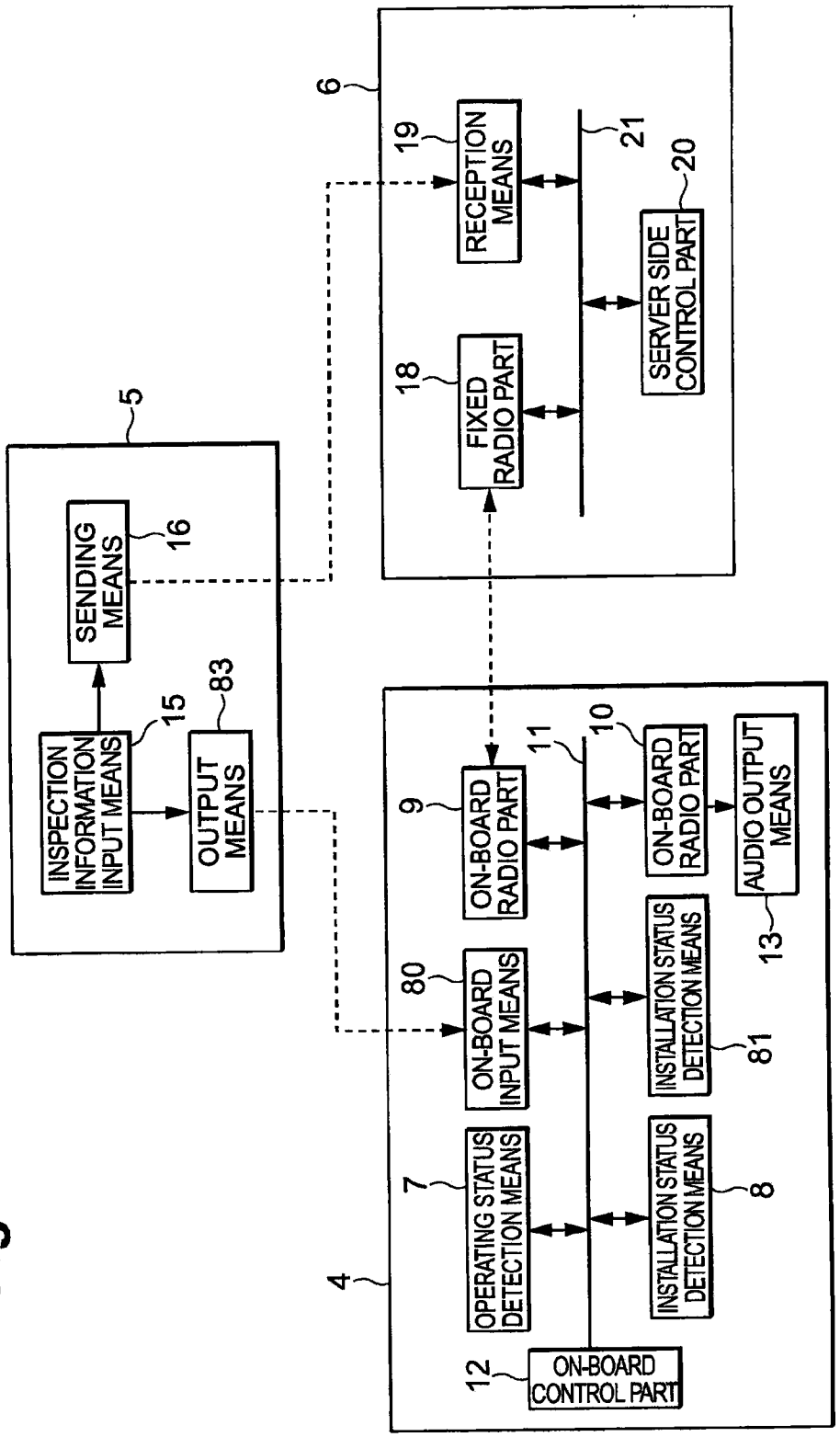

6
19
RECEPTION MEANS
21
20
SERVER SIDE CONTROL PART
18
FIXED RADIO PART
5
SENDING MEANS
16
INSPECTION INFORMATION INPUT MEANS
15
83
OUTPUT MEANS
9
ON-BOARD RADIO PART
11
10
ON-BOARD RADIO PART
AUDIO OUTPUT MEANS
13
80
ON-BOARD INPUT MEANS
INSTALLATION STATUS DETECTION MEANS
81
7
OPERATING STATUS DETECTION MEANS
INSTALLATION STATUS DETECTION MEANS
8
4
12
ON-BOARD CONTROL PART

Fig.8

Fig.9

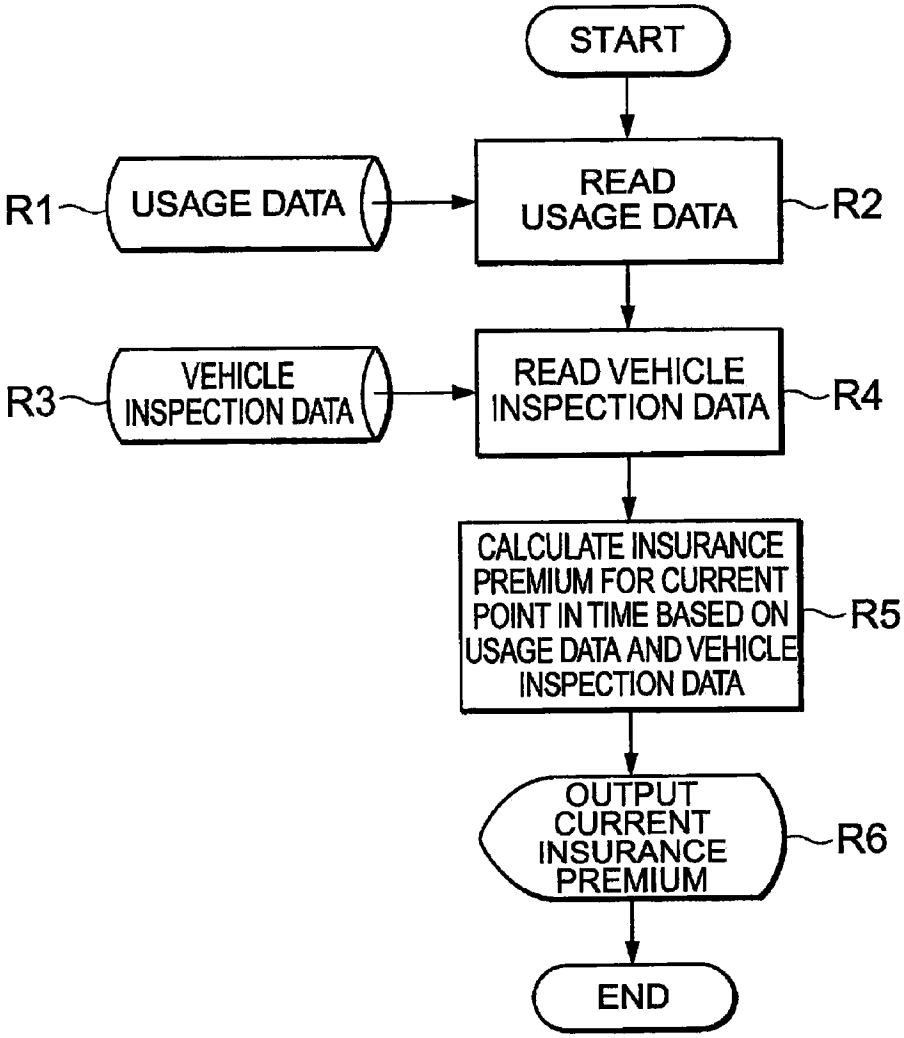
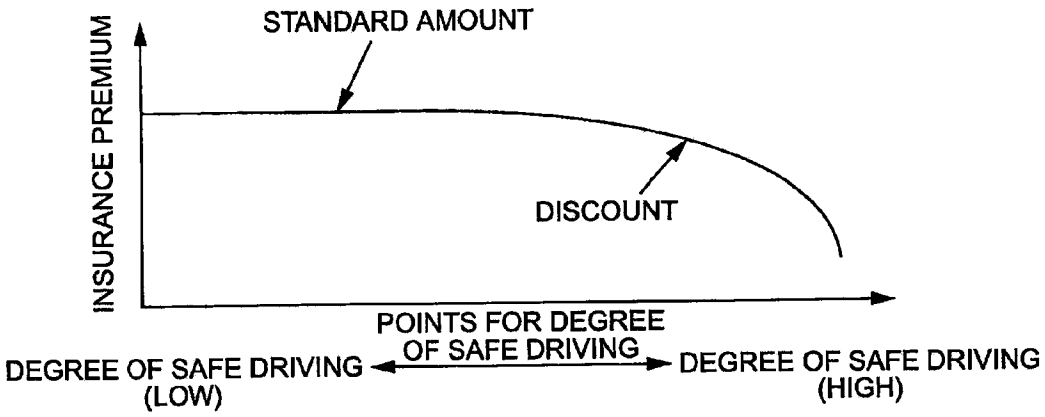

START
R1
USAGE DATA
READ USAGE DATA
R2
R3
VEHICLE INSPECTION DATA
READ VEHICLE INSPECTION DATA
R4
CALCULATE INSURANCE PREMIUM FOR CURRENT POINT IN TIME BASED ON USAGE DATA AND VEHICLE INSPECTION DATA
R5
OUTPUT CURRENT INSURANCE PREMIUM
R6
END

Fig.10


STANDARD AMOUNT
INSURANCE PREMIUM
DISCOUNT
POINTS FOR DEGREE OF SAFE DRIVING
DEGREE OF SAFE DRIVING (LOW)
DEGREE OF SAFE DRIVING (HIGH)

VEHICLE INSURANCE PREMIUM CALCULATION SYSTEM, ON-BOARD APPARATUS, AND SERVER APPARATUS

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention relates to a vehicle insurance premium calculation system that calculates the appropriate vehicle insurance premium by taking into account the maintenance and management status of the vehicle.

[0003] 2. Description of the Related Art

[0004] Related art, for example, includes a method and system for determining car insurance premiums based on the monitoring, recording, and communication of data showing the operating characteristics of the operator and vehicle as disclosed in Japanese Patent Application Laid-Open No. H11-515811. In this method and system, the insurance premium is adjusted retrospectively by linking operating characteristics to prescribed safety standards, and is then set for the future. This method includes a process that monitors a multiplicity of unprocessed data elements that show the actions of operators or how the car is being operated. Selected ones of these unprocessed data elements are recorded when it is determined that they have a prescribed relationship with a safety standard. Selected elements are combined so that any additional charge or discount that should be applied to the basic premium for car insurance can be specified when those elements are processed in an insurance company profile. The vehicle insurance premium is ultimately generated from the basic premium and any additional charges or discounts.

SUMMARY OF THE INVENTION

[0005] However, in the art described in the aforementioned publication, it has been difficult for a car insurance company to prove that a car has been properly maintained and serviced by a user (or driver) because the insurance premium is calculated based simply on information relating to the vehicle's operation and history of safety apparatus use. That is, it was not possible to calculate car insurance premiums that took into account whether or not components such as tires and brake pads, used to run a vehicle safely, have been serviced or maintained. This system aims to calculated appropriate vehicle insurance premiums by taking into account the maintenance and servicing history of the vehicle.

[0006] A first vehicle insurance premium calculation system comprises a usage status detection means that detects the usage status of a vehicle, a data input means through which data relating to vehicle servicing or maintenance is input, and an insurance premium calculation means that calculates vehicle insurance premiums based on the detection results and input data.

[0007] The usage status of a vehicle refers to the way in which a vehicle is operated by the driver or the installation status of equipment for protecting passengers. Thus, because the usage status of a vehicle is detected and vehicle insurance premiums are calculated to incorporate data relating to the vehicle maintenance and management, appropriate vehicle insurance premiums can be determined.

[0008] The first vehicle insurance premium calculation system can further comprise a display means that displays data relating to the calculated insurance premium.

[0009] Data relating to the calculated insurance premium is thus displayed and so the user (or driver) of a vehicle can be encouraged to drive safely, install safety equipment as appropriate, and properly maintain a vehicle.

[0010] The first vehicle insurance premium calculation system can further comprise an audio output means that outputs data relating to calculated insurance premiums by voice.

[0011] Data relating to the calculated insurance premium is thus output by voice and so the user (or driver) of a vehicle can be encouraged to drive safely, install safety equipment as appropriate, and properly maintain a vehicle.

[0012] A second vehicle insurance premium calculation system is a vehicle insurance premium calculation system comprising on-board apparatus, a maintenance data management means, and server apparatus. The onboard apparatus comprises a usage status detection means that detects the usage status of a vehicle, an on-board sending means that sends at least data relating to the detected usage status, an on-board reception means that receives at least data relating to insurance premiums, and an on-board display means that displays the received data. The maintenance data management means comprises a data input means that enters at least data relating to vehicle maintenance or management, and a data sending means that sends at least data relating to vehicle maintenance or management. The server apparatus comprises a reception means on the server side that receives data relating to the usage status and data relating to the maintenance or management of a vehicle, an insurance premium calculation means that calculates vehicle insurance premiums based on received data, and a sending means on the server side that sends data relating to the calculated insurance premiums to the on-board apparatus.

[0013] The usage status of a vehicle is thus detected and vehicle insurance premiums that incorporate data relating to vehicle maintenance or management are calculated. Therefore, appropriate vehicle insurance premiums can be determined.

[0014] A third vehicle insurance premium calculation system is a vehicle insurance premium calculation system that comprises on-board apparatus, a maintenance data management means, and server apparatus. The onboard apparatus comprises a usage status detection means that detects the usage status of a vehicle, an on-board input means that enters data relating to vehicle maintenance or management from the maintenance data management means, an insurance premium calculation means that calculates insurance premiums based on all detection results and data relating to vehicle maintenance or management, an on-board display means that displays data relating to calculated vehicle insurance premiums, and an on-board sending and reception means that sends at least data relating to the calculated vehicle insurance premiums. The maintenance data management means comprises a data input means that enters at least data relating to vehicle maintenance or management, and an output means that outputs at least data relating to vehicle maintenance or management. The server apparatus comprises a reception means on the server side that receives at least data relating to vehicle insurance premiums.

[0015] The vehicle usage status is thus detected and vehicle insurance premiums that incorporate data relating to vehicle maintenance and management are calculated. Therefore, suitable vehicle insurance premiums can be determined. Also, the insurance premiums calculated in the on-board apparatus can be managed by the server apparatus.

[0016] In any of the above vehicle insurance premium calculation systems, the insurance premium calculation means can be configured so that vehicle insurance premiums can be calculated in real time to suit fluctuations in data relating to detection results and vehicle maintenance or management data.

[0017] Vehicle insurance premiums are thus calculated in real time to match detection results and fluctuations in data relating to the maintenance or management of a vehicle and so users (or drivers) of that vehicle can always understand the changes to insurance premiums made based on fluctuations in data. That is, they can understand the increases in insurance premiums that result from unsafe driving or the decreases in insurance premiums that result from the proper installation of safety equipment. As a result, the user (or driver) of a vehicle can be encouraged to drive safely, properly install safety equipment, and properly maintain a vehicle.

[0018] In any of the above vehicle insurance premium calculation systems, the insurance premium calculation means can be configured to allow estimated vehicle insurance premiums to be calculated to suit detection results and fluctuations in the data relating to vehicle maintenance or management.

[0019] Estimated values for vehicle insurance premiums are thus calculated to suit detection results and fluctuations in data relating to vehicle maintenance or management. Therefore, each time estimated values are displayed, the user (or driver) of a vehicle can understand insurance premium estimates calculated based on data fluctuations. That is, they can understand any increase in insurance premium that results from unsafe driving or any decrease in insurance premium that results from the proper installation of safety equipment. As a result, the user (or driver) of a vehicle can be encouraged to drive safely, properly install safety equipment, and properly maintain a vehicle.

[0020] The on-board apparatus can also be configured to incorporate a usage status detection means that detects the usage status of a vehicle, a on-board sending means that sends at least data relating to the detected usage status, a on-board reception means that receives at least data relating to insurance premiums, and an onboard display means that displays the received data.

[0021] The usage status of a vehicle is thus detected and sent and data relating to insurance premiums calculated based on the sent data is displayed. Therefore, a user (or driver) of that vehicle can be encouraged to drive safely, properly install safety equipment, and properly maintain a vehicle.

[0022] One on-board apparatus can also be configured to incorporate a usage status detection means that detects the usage status of a vehicle, an on-board input means that enters data relating to the maintenance or management of a vehicle, an insurance premium calculation means that calculates the insurance premium for a vehicle based on detection results and data relating to the maintenance or management of the vehicle, and a on-board display means that displays data relating to the calculated vehicle insurance premiums.

[0023] The usage status of a vehicle is thus detected and the vehicle insurance premium, which incorporates data relating to vehicle maintenance or management, is calculated and so an appropriate vehicle insurance premium can be determined.

[0024] The server apparatus is configured to include a reception means on the server side that receives data relating to the usage status of a vehicle and data relating to the maintenance or management of a vehicle, an insurance premium calculation means that calculates the vehicle insurance premium based on received data, and a sending means on the server side that sends data relating to the calculated insurance premium.

[0025] Vehicle insurance premiums are thus calculated based on data relating to the usage status of a vehicle and data relating to the maintenance or management of the vehicle and so an appropriate vehicle insurance premium can be determined.

[0026] The vehicle insurance calculation method is configured to include a usage status detection process that detects the usage status of a vehicle, a data input process that enters data relating to vehicle maintenance or management, and an insurance premium calculation process that calculates vehicle insurance premiums based on detection results and input data.

[0027] The usage status of a vehicle is thus detected and a vehicle insurance premium, incorporating data relating to vehicle maintenance or management, is calculated and so an appropriate vehicle insurance premium can be determined.

[0028] The vehicle insurance premium calculation method can also include a display means that displays data relating to the calculated insurance premium.

[0029] Data relating to calculated insurance premiums is thus displayed and so a user (or driver) of that vehicle can be encouraged to drive safely, properly install safety equipment, and properly maintain a vehicle.

[0030] The vehicle insurance premium calculation method can also include a voice output process that outputs data relating to calculated insurance premiums by voice.

[0031] Data relating to calculated insurance premiums is thus output by voice and so a user (or driver) of that vehicle can be encouraged to drive safely, properly install safety equipment, and properly maintain a vehicle.

[0032] The vehicle insurance premium calculation system can also be configured with an operation status detection means that detects how a vehicle is being operated by a driver, an installation status detection means that detects the installation status of equipment for protecting passengers, an insurance premium calculation means that calculations vehicle insurance premiums based on the detection results, and a display means that displays the calculated vehicle insurance premiums for the driver.

[0033] This configuration detects how a vehicle is being operated by its driver and detects the installation status of equipment for protecting passengers. It then calculates

vehicle insurance premiums based on the results of such detection. This enables appropriate vehicle insurance premiums to be determined. Also, the calculated vehicle insurance premiums are displayed on the display means and so a user (or driver) of that vehicle can be encouraged to drive safely and properly install safety equipment.

[0034] This vehicle insurance premium calculation system can further incorporate a maintenance and management status detection means that detects the maintenance and management of a vehicle. The insurance premium calculation means can also be configured to calculate vehicle insurance premiums that incorporate the detected vehicle maintenance or management status.

[0035] Vehicle insurance premiums that incorporate data relating to vehicle maintenance or management are thus calculated and so appropriate vehicle insurance premiums can be determined. That is, maintenance of a vehicle, for example ensuring vehicle oils, tires, and brake pads are kept in good condition, is necessary to ensure that a vehicle runs safely and therefore appropriate insurance premiums can be determined by reflecting a vehicle's maintenance and management status in the insurance premiums. As a result, a user (or driver) of that vehicle can be encouraged to properly maintain a vehicle.

BRIEF DESCRIPTION OF THE DRAWINGS

[0036] **FIG. 1** shows a concept of a motor vehicle insurance premium calculation system according to a first embodiment;

[0037] **FIG. 2** is a block diagram showing an outline of the configuration of a car insurance premium calculation system according to a first embodiment;

[0038] **FIG. 3** is a flowchart showing the operations by which on-board apparatus collects various data;

[0039] **FIG. 4** is a flowchart showing the operations by which the maintenance data management means collects various data;

[0040] **FIG. 5** is a flowchart showing the operations by which motor vehicle insurance premiums are calculated;

[0041] **FIG. 6** shows an example of a screen display in step ST10 of **FIG. 5**;

[0042] **FIG. 7** shows an example of a screen display in step ST10 of **FIG. 5**;

[0043] **FIG. 8** is a block diagram showing an outline of the configuration of a car insurance premium calculation system according to a second embodiment;

[0044] **FIG. 9** is a flowchart showing the operation by which the insurance premium calculation means provided in the on-board apparatus calculates car insurance premiums; and

[0045] **FIG. 10** is a graph showing the relationship between insurance amounts and degrees of safe driving.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0046] The embodiments of the present invention will be explained below with reference to diagrams. In the vehicle insurance premium calculation system according to the present invention, items, mainly including people, objects, passengers, and vehicles, are considered to be the subject of insurance. The insurance is not limited to the type of "vehicle insurance" that applies only to damage to the vehicle body. In the embodiment that follow, the vehicle insurance premium calculation system according to the present invention is explained using an example of a car. However, the present invention is not limited to use with cars.

[0047] (First Embodiment)

[0048] **FIG. 1** shows the concept of the car insurance premium calculation system according to a first embodiment of the present invention. A user or driver of car **1** (hereinafter referred to as a "user") subscribes to car insurance handled by car insurance company **2**. When the user uses car **1**, an on-board apparatus (on-board) apparatus installed in car **1** collects, via various sensors, information relating to the operation of car **1** by the user and information relating to the installation status of safety equipment. The collected information is provided from the on-board apparatus to the car insurance company **2**. Here, the car **1** is a mobile object and so radio communication is used between car **1** and car insurance company **2**.

[0049] A contract repair factory **3**, which has a contractual relationship with car insurance company **2**, knows whether or not the user of car **1** has regularly inspected and serviced car **1**. When the inspection and service of car **1** is carried out at contract repair factory **3**, that information is sent to car insurance company **2**. Radio communication or wired communication can be used to report that information.

[0050] Car insurance company **2** calculates the car insurance premiums based on information sent by radio communication from car **1** and information sent from contract repair factory **3**. For example, when a user has properly installed safety equipment in car **1**, drives car **1** safely, and properly maintains and manages car **1** at contract repair factory **3**, car insurance company **2** assumes a reduction in any insurance that may have to be paid out for car **1**. Therefore, the insurance premiums payable for car **1** are discounted. Conversely, if the user **1** has not properly installed safety equipment in car **1**, does not drive safely, and does not properly maintain or manage car **1**, car insurance company **2** assumes an increase in any insurance that may have to be paid out for car **1**. Therefore, the car insurance premiums payable for that car are increased. Data relating to the car insurance premiums after any discount or increase has been applied is sent via radio communication from car insurance company **2** to car **1**. The received data relating to the car insurance premium is displayed so that it is visible to the user of car **1**.

[0051] The user of car **1** can judge whether or not they are driving car **1** safely, whether or not they have properly installed safety equipment, and whether or not they are properly maintaining or managing car **1** from the displayed car insurance premium. That is, an increase in the displayed car insurance premium encourages the user to drive the vehicle safely, properly install safety equipment, and properly maintain the car. This can heighten their awareness of traffic safety. On the other hand, a decrease in the premium makes the user aware that their actions thus far are appropriate and enables them to receive a decrease in insurance premiums. Also, by increasing the awareness of users about

traffic safety, car insurance company **2** can reduce the amount of insurance that it must pay out. Furthermore, by being provided with the opportunities for regular inspections and servicing, the contract repair factory **3** can increase their profits.

[0052] **FIG. 2** is a block diagram showing an outline of the configuration of a car insurance premium calculation system according to a first embodiment of the present invention. The car insurance premium calculation system according to the first embodiment comprises an on-board apparatus **4** loaded into car **1**, a maintenance data management means **5** provided in the contract repair factory **3**, and server apparatus **6** installed in the car insurance company.

[0053] The on-board apparatus **4** comprises an operation status detection means (detector) **7** that detects how a car is being operated by a user, an installation status detection means (detector) **8** that detects whether or not equipment for protecting passengers has been installed, an on-board radio part **9** that sends and receives data by radio, and a display means **10** that displays data so that it is visible. These are then connected via a control bus **11** to a on-board control part (processor) **12**. In the present invention, the operating status of a car by a user, or the installation status of equipment for protecting passengers is expressed as the "vehicle usage status".

[0054] The operating status detection means **7** consists of various sensors. It detects how the accelerator is used by the user of car **1**, the speed at which the car is driven, how the anti-lock braking (or brake) system (ABS) is working, the time, changes in engine revolutions, transmission settings (parking, reverse, drive, neutral), and use of left and right indicators and of headlamps. It then outputs this information as data. It can detect the current location of a car using a global positioning satellite (or system) (GPS) and uses a G sensor to detect deceleration and acceleration and braking. Furthermore, using an air analyzer or breath tester, this means can detect whether or not a user has consumed alcohol and the levels consumed. The operating status detection means **7** also includes various sensors for collecting information relating to the operating status of car **1**.

[0055] The installation status detection means **8** consists of various sensors that detect the installation status of safety equipment. It detects seatbelts installation status, child seat installation status, and the position in which head rests are used and outputs information as data. In other words, this detector **8** detects passenger activation status of protection equipment for passengers. Using passenger detection sensors, the wearing status detection means **8** detects the angle of seat backs and the positions in which passengers are seated. It checks that child seats in passenger seats equipped with passenger seat air bags are installed facing backwards. Here, the phrase installation status refers not simply to whether or not safety devices are being used but also to whether or not they have been properly installed. That is, even if a seat belt is being used it cannot be said to be being used properly if the shoulder anchor for the seatbelt is set so that the seatbelt does not go over the shoulder of a passenger. A method using image recognition can be used to detect whether safety equipment has been installed properly. That is, an image taken of a passenger from the front is entered and by recognizing the position of eyes and shoulders from the image, the detection means an detect whether or not the height of the shoulder anchor on the seat belt has been properly adjusted. The installation status detection means **8** includes all sensors for collecting other information relating to the installation status of safety equipment in car **1**.

[0056] Data collected by the operating status detection means **7** and installation status detection means **8** is sent to the on-board radio part **9** via a control bus **11** while control by the on-board control part **12** is being received. The on-board radio part **9** sends data detected as above to server apparatus **6**, installed at the car insurance company **2**, via radio.

[0057] The display means **10** consists, for example, of a liquid crystal monitor, and displays video, static images, and writing in a visible format. The display means **10** also has a voice output means **13** that outputs data by voice. This means that voice guidelines or sound effects are output with the screen display in display means **10**. The voice output means **13** comprises, for example, an amp part, CD player, DVD player, CD-ROM drive, MP3 player, and stereo speakers. Audio or voice data can be replayed and output.

[0058] The on-board control part **12** controls the entire on-board apparatus **4**. Also, the on-board control part **12** contains memory that is not pictured. This memory stores data collected by operating status detection means **7** and installation status detection means **8** and data received via radio by the on-board radio part **9**.

[0059] The contract repair factory **3** has a maintenance data management means **5**. This manages data relating to whether or not car **1** has been properly maintained or managed when the user of car **1** brings car **1** to the control repair factory **3**. The maintenance data management means **5** comprises an inspection information input means **15** that enters data relating to the maintenance or management of the car and a sending means **16** that uses radio or wired means to send data relating to car maintenance or management.

[0060] The inspection information input means **15** enters the results of an inspection of components that need replacement regularly or after a certain amount of use in car **1**. Also, this inspection information input means **15** mainly detects items that cannot be detected by on-board apparatus **4**. For example, information such as the condition of the various oils, the conditions of brake pads, engine timing belt, brake drum, and tires, and any replacements made when these have deteriorated, is input as data. The inspection information input means **15** also has memory that is not pictured in which the input data is stored. Also, the data entered in the inspection information input means **15** is sent to server apparatus **6** at the car insurance company **2** using sending means **16**. Here, sending means **16** can send data by radio or by wired means.

[0061] Server apparatus **6** is installed in the car insurance company **2**. The server apparatus **6** calculates an appropriate car insurance premium based on data received from the on-board apparatus **4** and the maintenance data management means **5**. It then sends the calculated car insurance premium to the on-board apparatus **4**. That is, server apparatus **6** comprises a fixed radio part **18** that sends and receives data by radio, a reception means **19** that receives data relating to car maintenance or management from sending means **16** by radio or wired communication, and insurance premium calculation means (processor) **20** that calculates car insur-

ance premiums based on detection results sent from on-board apparatus **4** and on car maintenance or management data sent from sending means **16**. These are also connected to the control part **22** on the server side via a control bus **21**. The control part **22** on the server side is equipped with memory, which is not pictured, and data relating to car insurance subscribers is stored in this memory as "user data".

[0062] The car insurance premium calculated by insurance premium calculation means **20** is controlled by the controller part **22** on the server side as data and is sent to a fixed radio part **18** via control bus **21**. The fixed radio part **18** sends car insurance premium data by radio to an on-board radio part **9** installed in the onboard apparatus **4**. Car insurance premium data received by the on-board radio part **9** is displayed on display means **10** and at the same time prescribed voice data is output by the voice output means **13**.

[0063] Next, the operations in a car insurance premium calculation system according to the first embodiment as configured above will be explained. **FIG. 3** is a flowchart that shows an operation in which various data is collected by on-board apparatus **4**. The on-board control part **12** in the on-board apparatus **4** determines whether or not information collection will start (step S1). Information collection will start, for example, when the user inserts a key in the ignition switch and turns it to the accessory position, when the running speed reaches a prescribed value, or when the running speed drops below a prescribed value. Here, it is assumed that information collection starts when the user inserts a key in the ignition switch and turns it to the accessory position.

[0064] In step S1, when the key is not in the accessory position, the judgement made in step S1 is repeated. When the key is turned as far as the accessory position, a prompt from the on-board control part **12** will ensure that collection of information from various sensors will be started by the operating status detection means **7** and the installation status detection means **8** (step S2). The operating status detection means **7** uses various sensors to detect how a user is operating car **1**. For example, is detects how the accelerator is being used, the running speed, use of ABS, the time, changes in engine revolutions, transmission settings, use of left and right indicators, and use of headlamps and outputs this information as data. Also, the installation status detection means **8** uses various sensors to detect the installation status of safety equipment. For example, it detects the installation status of seatbelts, detects the installation status of child seats, and detects the positions in which headrests are being used. It then outputs this information as data.

[0065] In step S2, the on-board control part **12** determines whether the operation and installation statuses of a vehicle are safe or dangerous based on data collected from operating status detection means **7** and installation status detection means **8**. When it determines that both the operating and installation statuses are safe, the degree of safe operation is recorded in point form (step S3). When it determines that the statuses are dangerous, the danger status is recorded in point form (step S4). The data stored in steps S3 and S4 are stored in the memory provided in the on-board control part **12** as "usage data" (step S5).

[0066] Next, the on-board control part **12** determines whether or not information collection will end (step S6). When information collection has not ended, processing moves to step S2. When it has ended, processing ends.

[0067] Next, collection of information in the contract repair factory **3** will be explained. **FIG. 4** is a flowchart showing the operation in which the maintenance data management means **5** in the contract repair factory **3** collects various data. When the user of car **1** brings car **1** to contract repair factory **3** and requests an inspection or service, inspection of car **1** by a worker begins. Firstly, inspection information relating to the user and car **1** (for example, details of car inspection certificate and details of car insurance) and identification information is entered (step T1). When verification of the user and car **1** has been obtained, data relating to the results of an inspection or service is entered via the inspection information input means **15**. The inspection information input means **15** mainly detects items that are not detected in the on-board apparatus **4**. For example, information such as the cleanliness of the various oils, and the state of brake pads, engine timing belts, brake drums and tires, and any replacement of deteriorated parts is entered as data. Also, the data entered in the memory provided within the inspection information input means **15** is recorded. The entered data relating to the results of inspections and services is sent to server apparatus **6** by sending means **16** (step T2).

[0068] In the server apparatus **6**, the reception means **19** receives the data relating to the results of an inspection or service (step T3). That data is recorded in the memory provided inside the control part **22** on the server side. Here, the control part **22** on the server side updates the "user data" recorded in memory that corresponds to the received ID (step T4). Processing ends when the update ends.

[0069] Next, the operation in which the server apparatus **6** calculates the car insurance premiums will be explained. **FIG. 5** is a flowchart that shows the operation in which the car insurance premium calculation means **20** in server apparatus **6** calculates car insurance premiums. Firstly, in the on-board apparatus **4**, "usage data" is read from the memory in the on-board control part **12** (steps ST1 and ST2). The on-board radio part **9** sends the usage data thus read and an ID to the server apparatus **6** (step ST3). The server apparatus **6** receives the usage data and ID sent by the fixed radio part **18** (step ST4). The control part **22** on the server side updates that "user data" stored in memory that corresponds to received IDs (steps ST5 and ST6). This means that the latest data collected in the on-board apparatus **4** and the latest data collected at the contract repair factory **3** is stored in the memory in the control part **22** on the server side as "user data".

[0070] Next, the insurance premium calculation part **20** reads the "user data" corresponding to the ID from the memory in the control part **22** on the server side and calculates the insurance premium for the next term (step ST7). Here, the "insurance premium for the next term" refers to the insurance premium for the next day when the premium is calculated on a daily basis, the insurance premium for the next month when the premium is calculated on a monthly basis, and the insurance premium for the next year when the premium is calculated on an annual basis. This enables a flexible selection to suit the way in which the user uses insurance.

[0071] Also, the insurance premium can be calculated in real time as the data collected from the on-board apparatus **4** and contract repair factory **3** changes. Furthermore, estimated values for insurance premiums can be calculated as the data changes.

[0072] The insurance premium calculation means **20** calculates insurance premiums by discounting or increasing them using a prescribed value as a standard. Specifically, when the user data includes data relating to speeding and the length of time for which speeding occurs, non-use or inappropriate use of seatbelts, application of ABS other than during an accident, sudden acceleration and deceleration, or data showing that brake pads have not been replaced despite being worn, processing will occur to increase the standard insurance premium by a certain percentage and calculate an increased premium. In contrast, when the user data includes data relating to driving within the speed limit, appropriate use of seatbelts and head rests, and appropriate replacement of brakes and hoses, processing will occur to discount the standard insurance premium by a certain percentage and calculate a discounted premium.

[0073] When the insurance premium calculation means **20** has calculated the car insurance premium, it receives control from the control part **22** on the server side and the fixed radio part **18** sends, by radio, the data relating to the calculated car insurance premium to the on-board apparatus **4** (step ST8). The on-board apparatus **4** receives the data relating to the car insurance premium sent by the on-board radio part **9** (step ST9). It receives control from the on-board control part **12** and the display means **10** displays the data relating to the car insurance premium (step ST10).

[0074] **FIG. 6** shows an example of a screen display in step ST10 of **FIG. 5**. This screen displays pass rates for each item and insurance premium discounts estimated at the end of the month. These are based on data relating to safety equipment that has been collected from the start of the month to the present. That is, this figure is an example of what is displayed at the end of each month when the operation and installation statuses for one month are calculated in numeric form and reflected in the amount by which insurance premium is multiplied. As shown in **FIG. 6**, between November 1 and 18 in a particular year, the pass rate for seatbelt installation, height adjustment of the seatbelt shoulder anchor, and installation of child seats was 100%. However, the pass rate for headrest height adjustment was 30% and the pass rate for seat back angle adjustment was 80%. Based on these figures, as of November 18 the estimated discount on the insurance premium at the end of the month is shown to be 3% of the standard figure. Also shown is the discount of 5% that would apply if all the pass rates were 100%. This suggests to the user that there is room for improvement.

[0075] Estimated values for car insurance premiums are thus calculated to suit detection results and any changes in data relating to car maintenance or management. Therefore, each time estimated values are displayed, the user of that car can understand that estimated insurance premiums are calculated based on changes in data. That is, the user can understand an increase in insurance applied because of unsafe driving and a discount applied when safety equipment is properly installed. As a result, the user of that car is encouraged to drive safely, properly install safety equipment, and properly maintain the car.

[0076] **FIG. 7** shows an example of a screen display in step ST10 in **FIG. 5**. Here, user operating levels and discounts rates for insurance premiums up until the previous month are shown in graph form based on data relating to the driving operation of the car from the start of the month to the present. That is, at the end of each month, the evaluation of operating levels for one month is calculated in numeric form and displayed to reflect the amount by which the insurance premium will be multiplied. The operating levels show driving techniques and the level of safe driving as points which are then evaluated as numbers. For example, in the evaluation of driving techniques, G sensors installed in a car are used to detect whether or not deceleration occurs smoothly without any locking of tires and whether or not curves in the road are handled without unreasonable steering. The findings are then converted into points. In the evaluation of safe driving, inter-car distance sensors are used to detect whether or not a safe distance is being maintained between vehicles to suit the running speed. The finding is then converted into points. The operation level, as shown in points, is displayed as a bar graph as shown in **FIG. 7**. It can be seen that operating levels improved in September when compared to May. The discount rates applied to the insurance are displayed in a broken line graph. Thus it can be seen that as operating levels improve, the discount applied to the insurance increases and the car insurance premium payable by the user decreases.

[0077] In **FIG. 6** above, the discount to be applied to the insurance is calculated on a monthly basis. In **FIG. 7**, although operating levels are calculated for one month, they can also be displayed in real time as detection results and data relating to car maintenance or management change. That is, by calculating the car insurance premiums in real time to suit changes in detection results and data relating to car maintenance or management, the system enables the user of the car to always understand that insurance premiums are calculated based on changes in data. That is, the user can understand that increases are applied to insurance premiums when unsafe driving occurs and that discounts apply when safety equipment is properly installed. As a result, the user of a car can be encouraged to drive safely, properly install safety equipment, and properly maintain the car.

[0078] Also, in step ST10 in **FIG. 5**, in addition to displaying the car insurance premium or estimate on the screen it is also possible to display the actions that lead to any increase in premium in video form. For example, in the check items shown in **FIG. 6**, the pass rate for headrest adjustment was low. Therefore, a movie can be run to show the injuries that can result in a collision when headrest heights are not suitably adjusted.

[0079] When a movie is displayed, the voice output means **13** will replay the sounds of tires squealing with sudden braking, the sound of another car colliding into the rear of the car, and a person's voice yelling out, "Watch out!" as audio data to reinforce the dangerous situation to the user. After the dangerous situation is displayed, a video and written and audio information will be used to guide a user into correct use of the head rests. In another example, a movie is shown if the timing belt, which is in the engine and needs replacement when a car has been driven for more than a certain distance, is not replaced. The problems that could occur in the car are displayed on the screen along with voice output to reinforce the need for replacement to the user. A

movie urging the driver to replace the timing belt will also be displayed. It is preferable that a DVD player, which can incorporate large amounts of recorded data and in which processing is fast, is used to replay such movies and audio data.

[0080] Thus, not only is information provided visually in the display means **10** but also audio data is output by the audio output means **13**. Therefore, it is possible to effectively encourage the users of a car to drive safely, properly install safety equipment, and properly maintain the car.

[0081] As described above, the car insurance premium calculation system according to the first embodiment of the present invention enables detection of the way in which a user operates car **1** and the installation status of equipment that protects passengers. A car insurance premium that incorporates data relating to the maintenance or management of car **1** is then calculated to enable determination of an appropriate car insurance premium. That is, since constant maintenance of oils, tires, and brake pads in a good condition in car **1** is required for the safe driving of car **1**, an appropriate insurance premium can be determined by reflecting the maintenance and management status of car **1** in the insurance premium. The calculated insurance premium is sent to car insurance company **2** by radio communication from car **1** and is displayed on display means **10** in the on-board apparatus **4**. Therefore, the user of car **1** can be encouraged to drive safely, properly install safety equipment, and properly maintain car **1**.

[0082] In the first embodiment, an example in which the on-board apparatus **4** and maintenance data management means **5** each send collected data via independent paths to server apparatus **6** was explained. However, the present invention is not limited to this embodiment. That is, the on-board apparatus **4** can also combine data it has collected independently with data entered from the maintenance data management means **5** and send both to server apparatus **6**.

[0083] Also, maintenance data management means **5** can combine data it has collected independently with data collected from the on-board apparatus **4** and send it to server apparatus **6**. For example, a radio part can be installed in the maintenance data management means **5** to facilitate communication with the on-board apparatus **4**. This enables reception by radio of data collected by the on-board apparatus **4**. When a car in which a onboard apparatus **4** is installed is inspected at a contract repair factory **3**, the maintenance data management means **5** combines maintenance data and data collected by the on-board apparatus **4** then sends that data to server apparatus **6**. This enables calculation of car insurance premiums in the server apparatus **6** regardless of the path by which data has travelled.

[0084] (Second Embodiment)

[0085] **FIG. 8** is a block diagram showing an overview of the configuration of a car insurance premium calculation system according to a second embodiment of the present invention. As opposed to the first embodiment, in the second embodiment the insurance premium calculation means is removed from server apparatus **6**. Instead, an insurance premium calculation means (processor) **81** is installed in the on-board apparatus **4**. That is, insurance premiums are calculated independently in the on-board apparatus **4** based on collected information. Furthermore, an onboard input means **80**, which is used to accept the entry of inspection information from contract repair factory **3**, is installed in the on-board apparatus **4**. Memory, not pictured, in which input data is recorded is provided in the on-board input means **80**. An output means **83** is provided in the maintenance data management means **5** of the contract repair factory **3** to send entered points information to the on-board apparatus **4**. The rest of the configuration is the same as that in the above first embodiment and so explanation of it will be omitted here.

[0086] Next, the operations of a car insurance premium calculation system according to the second embodiment as configured above will be explained. As in the first embodiment, the on-board control part **12** determines whether the operating status and installation status are dangerous or safe based on data collected by the operating status detection means **7** and installation status detection means **8**. If both operation and installation statuses are safe, the degree of safe operation is recorded. If dangerous, the danger status is recorded. Data thus recorded is stored as "usage data" in the memory installed in the vehicle control part **12**.

[0087] At the contract repair factory **3**, when the user of car **1** brings car **1** to the contract repair factory **3** for inspection or a service, inspection of car **1** by a worker starts. The worker enters data relating to the results of the inspection and service via the inspection information input means **15**. As in the first embodiment, the inspection information input means **15** mainly detects matters that are not detected in the on-board apparatus **4**. The detected inspection information is sent by output means **83** to on-board input means **80**. Here, communication between the output means **83** and onboard input means **80** can be conducted using radio or wired communication and a memory card can be used in on-board input means **80** for reading the inspection information after it has been recorded. The entered inspection information is stored as "vehicle inspection data" in the internal memory provided in on-board input means **80**.

[0088] Data collected in the contract repair factory **3** can also be sent to server apparatus **6** via sending means **16**. When the reception means **19** in server apparatus **6** receives the sent data, the car insurance company also has an understanding of how the car is being maintained.

[0089] **FIG. 9** is a flowchart showing the operations involved when the insurance premium calculation means **81** provided in on-board apparatus **4** calculates car insurance premiums based on the data collected as above. The on-board control part **12** reads "usage data" from internal memory and sends it to insurance premium calculation means **81** (steps R1 and R2). In the second embodiment, the "usage data" allows information on the safe operation of a vehicle up to the present to be obtained.

[0090] Also, the on-board input means **80** reads "vehicle inspection data" from internal memory and sends it to insurance premium calculation means **81** (steps R3 and R4). In the second embodiment, "vehicle inspection data" allows information regarding inspections, services, and component replacements received by car **1** in the past to be obtained.

[0091] Insurance premium calculation means **81** calculates the car insurance premium for the current point in time based on usage data and vehicle inspection data (step R5). In the second the embodiment, the car insurance premium is calculated based on the standard curve shown in **FIG. 10**.

[0092] **FIG. 10** is a graph showing the relationship between insurance amounts and points awarded for degrees of safe operation. As shown in **FIG. 10**, premiums are low when the points for safe operation are low. When the points for degree of safe operation exceed a prescribed threshold, discounting of the insurance premium occurs to suit the curve shown in **FIG. 10**.

[0093] When the current insurance premium is calculated by insurance premium calculation means **81**, as in the first embodiment, the premium is displayed on the display means **10** using video, static images, and writing (step R6). At the same time, audio data is replayed by audio output means **13**. Furthermore, the calculated insurance premium data is sent via radio by the on-board radio part **9** to the fixed radio part **18** in server apparatus **6**.

[0094] Thus, the car insurance premium calculation system, according to this second embodiment, detects the way in which car **1** is operated by a user and the installation status of equipment installed to protect passengers. Furthermore, it calculates car insurance premiums that incorporate data relating to the maintenance or management of car **1** and so accurate car insurance premiums can be determined. That is, good maintenance of the oils, tires and brake pads in car **1** is required for the safe driving of car **1** and so accurate insurance premiums can be determined by reflecting the maintenance and management status of car **1** in the insurance premium. Also, maintenance and management data for car **1** is directly input into on-board apparatus **4** and the on-board apparatus **4** calculates the car insurance premium. This means that processing can be fully completed within on-board apparatus **4**. In addition, less radio communication with the car insurance company **2** is required. Also, because the calculated insurance premiums are displayed on the display means **10** provided in the on-board apparatus **4**, the user of car **1** can be encouraged to drive safely, wear safety devices in an appropriate manner, and maintain car **1** appropriately. Furthermore, the calculated insurance premiums are sent by radio from the on-board apparatus **4** to car insurance company **2** and so the car insurance company **2** can understand the fluctuating insurance premiums.

[0095] In the example described in the explanation of the second embodiment, the calculated car insurance premiums are sent from the on-board apparatus **4** to server apparatus **6**. However, data collected from the operating status detection means **7** and installation status detection means **8** can also be sent from the onboard apparatus **4** to server apparatus **6** in parallel to this. When server apparatus **6** thus obtains data collected at the contract repair factory **3** and data collected in on-board apparatus **4**, the car insurance company **2** can obtain all the data backing up the car insurance premium sent from the on-board apparatus **4**.

[0096] Furthermore, by providing an insurance calculation means that calculates car insurance premiums in the server apparatus **6** as well, the car insurance company **2** can also calculate car insurance premiums. This enables the car insurance company **2** to check the car insurance premium sent from the on-board apparatus **4** and the car insurance premium it has calculated independently.

What is claimed is:

1. A vehicle insurance premium calculation system comprising:

usage status detection means for detecting usage status of a vehicle;

data input means for inputting data relating to maintenance or management of said vehicle; and

insurance premium calculation means for calculating vehicle insurance premium based on said inputted data and results of said detection.

2. The vehicle insurance premium calculation system according to claim 1, further comprising display means for displaying data relating to said calculated insurance premium.

3. The vehicle insurance premium calculation system according to claim 1, further comprising voice output means for enabling voice output of data relating to said calculated insurance premium.

4. The vehicle insurance premium calculation system according to claim 1, wherein said insurance premium calculation means calculates a vehicle insurance premium in real time in accordance with results of said detection and fluctuations in data relating to maintenance or management of said vehicle.

5. The vehicle insurance premium calculation system according to claim 1, wherein said insurance premium calculation means calculates an expected vehicle insurance premium in accordance with results of said detection and fluctuations in data relating to maintenance or management of said vehicle.

6. A vehicle insurance premium calculation system comprising an on-board apparatus, maintenance data management means, and a server apparatus:

wherein said on-board apparatus comprises:

usage status detection means for detecting usage status of a vehicle;

on-board sending means for sending at least data relating to said detected usage status;

on-board reception means for receiving at least data relating to insurance premiums; and

means for displaying said received data;

wherein said maintenance data management means comprises:

data input means for inputting at least data relating to maintenance or management of said vehicle; and

data sending means for sending at least data relating to maintenance or management of said vehicle; and

wherein said server apparatus comprises:

server side reception means for receiving data relating to said usage status and data relating to said maintenance or management of vehicle;

insurance premium calculation means for calculating vehicle insurance premiums based on said received data; and

server side sending means for sending data relating to said calculated insurance premiums to said on-board apparatus.

7. A vehicle insurance premium calculation system comprising an on-board apparatus, maintenance data management means, and a server apparatus:

wherein said on-board apparatus comprises:

usage status detection means for detecting usage status of a vehicle;

on-board input means for inputting data relating to maintenance or management of said vehicle from said maintenance data management means;

insurance premium calculation means for calculating vehicle insurance premiums based on results of said detection and data relating to maintenance or management of said vehicle;

on-board display means for displaying data relating to said calculated vehicle insurance premiums; and

on-board sending and reception means for sending at least data relating to said calculated vehicle insurance premiums;

wherein said maintenance data management means comprises:

data input means for inputting at least data relating to maintenance or management of said vehicle; and

output means for outputting at least data relating to maintenance or management of said vehicle; and

wherein said server apparatus comprises server side reception means for receiving at least data relating to said vehicle insurance premiums.

8. On-board apparatus, comprising:

usage status detection means for detecting usage status of a vehicle;

on-board sending means for sending at least data relating to said detected usage status;

on-board reception means for receiving at least data relating to insurance premiums; and

on-board display means for displaying said received data.

9. On-board apparatus, comprising:

usage status detection means for detecting usage status of a vehicle;

on-board input means for inputting data relating to the maintenance or management of said vehicle;

insurance premium calculation means for calculating vehicle insurance premiums based on results of said detection and data relating to maintenance or management of said vehicle; and

on-board display means for displaying data relating to said calculated vehicle insurance premiums.

10. Server apparatus, comprising:

server side reception means for receiving data relating to usage status of a vehicle and data relating to maintenance or management of said vehicle;

insurance premium calculation means for calculating vehicle insurance premiums based on said received data; and

server side sending means for sending data relating to said calculated insurance premiums.

11. A vehicle insurance premium calculation method, comprising:

a usage status detection step of detecting usage status of a vehicle;

a data input step of inputting data relating to maintenance or management of said vehicle; and

an insurance premium calculation step of calculating vehicle insurance premiums based on said detection results and said inputted data.

12. The vehicle insurance premium calculation method according to claim 11, wherein said insurance premium calculation step calculates a vehicle insurance premium in real time in accordance with results of said detection and fluctuations in data relating to maintenance or management of said vehicle.

13. The vehicle insurance premium calculation method according to claim 11, wherein said insurance premium calculation step calculates an expected vehicle insurance premium in accordance with results of said detection and fluctuations in data relating to maintenance or management of said vehicle.

14. The vehicle insurance premium calculation method according to claim 11, comprising a display step of displaying data relating to said calculated insurance premium.

15. The vehicle insurance premium calculation method according to claim 11, comprising a voice output step of enabling voice output of data relating to said calculated insurance premium.

16. A vehicle insurance premium calculation system, comprising:

operation status detection means for detecting how a vehicle is operated by a driver;

status detection means for detecting passenger activation status of protection equipment for passengers;

insurance premium calculation means for calculating vehicle insurance premiums based on results of said detection; and

display means for displaying said calculated vehicle insurance premium for said driver.

17. The vehicle insurance premium calculation system according to claim 16, further comprising maintenance or management status detection means for detecting maintenance or management status of vehicle, and wherein said insurance premium calculation means calculates vehicle insurance premium also based on said detected maintenance and management status of vehicle.

18. A vehicle comprising an on-board apparatus, said apparatus having:

usage status detection means for detecting usage status of the vehicle;

on-board sending means for sending at least data relating to said detected usage status;

on-board reception means for receiving at least data relating to insurance premiums; and

on-board display means for displaying said received data.

19. A vehicle comprising an on-board apparatus, said apparatus having:

usage status detection means for detecting usage status of a vehicle;

on-board input means for inputting data relating to the maintenance or management of said vehicle;

insurance premium calculation means for calculating vehicle insurance premiums based on results of said detection and data relating to maintenance or management of said vehicle; and

on-board display means for displaying data relating to said calculated vehicle insurance premiums.

20. A maintenance data management apparatus provided in a contract repair factory, said apparatus comprising:

an inspection information input means for entering data relating to a maintenance or management of the vehicle; and

a sending means for sending data received from said inspection information input means.

21. On-board apparatus, comprising:

a processor;

a detector that detects usage status of a vehicle, connected to said processor;

a radio part that sends data from said detector or said processor, said radio part receiving data relating to insurance premiums, said radio part being connected to said processor;

a display connected to said processor.

22. A vehicle insurance premium calculation system comprising an on-board apparatus of claim 21 and a server that sends data to and receives data from said radio part of said on-board apparatus.

23. On-board apparatus, comprising:

a detector that detects usage status of a vehicle;

an input device that accept the entry of inspection information from a contract repair factory

a processor connected both of said detector and said input device, being calculating insurance premiums based on input data;

a display connected to said processor.

24. A server that receives data relating to usage status of a vehicle and data relating to maintenance or management of said vehicle, comprising:

a processor that calculates vehicle insurance premiums based on said received data; and

a radio part that sends data relating to said calculated insurance premiums.

25. A vehicle insurance premium calculation system, comprising:

a first detector that detects how a vehicle is operated by a driver;

a second detector that detects passenger activation status of protection equipment for passengers;

a processor that calculates vehicle insurance premiums based on results of said detections; and

a display connected to said processor.

* * * * *

Exhibit 3

US006052466A

United States Patent [19]

Wright

[11] Patent Number: 6,052,466

[45] Date of Patent: Apr. 18, 2000

[54] **ENCRYPTION OF DATA PACKETS USING A SEQUENCE OF PRIVATE KEYS GENERATED FROM A PUBLIC KEY EXCHANGE**

[75] Inventor: **Andrew S. Wright**, Vancouver, Canada

[73] Assignee: **Telefonaktiebolaget L M Ericsson (publ)**, Stockholm, Sweden

[21] Appl. No.: **08/919,728**

[22] Filed: **Aug. 28, 1997**

[51] **Int. Cl.**[7] **H04L 9/22**

[52] **U.S. Cl.** **380/262**; 380/285; 380/44

[58] **Field of Search** 380/21, 48, 30, 380/44, 254, 260, 262, 265, 278, 282, 283, 285

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,200,770	4/1980	Hellman et al. .	
4,218,582	8/1980	Hellman et al. .	
4,956,863	9/1990	Goss	380/30
5,148,485	9/1992	Dent	380/46
5,222,140	6/1993	Beller et al. .	
5,253,294	10/1993	Maurer	380/21
5,299,263	3/1994	Beller et al. .	
5,319,712	6/1994	Finkelstein et al. .	
5,438,622	8/1995	Normile et al. .	
5,515,441	5/1996	Faucher .	
5,546,464	8/1996	Raith et al.	380/48

FOREIGN PATENT DOCUMENTS

2 681 165	of 0000	France .
24 14 144	of 0000	Germany .
2 297 016	7/1996	United Kingdom .

OTHER PUBLICATIONS

Diffie, "The First Ten Years of Public-Key Cryptography", Proceedings of the IEEE vol. 76, No. 5, May 1988.

European Patent Office, Standard Search Report, Jun. 10, 1998, File No. RS 100645 US.

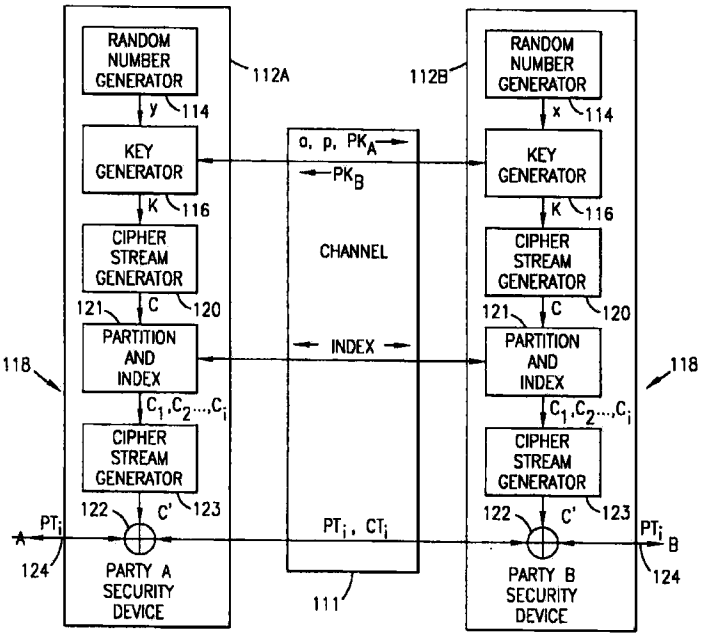
Primary Examiner—Gilberto Barron, Jr.

Attorney, Agent, or Firm—Jenkens & Gilchrist P.C.

[57] **ABSTRACT**

A first cipher stream generated from a private key negotiated as a result of a public key exchange is partitioned to form a sequence of secondary keys. The secondary keys are then indexed. In one instance, each plaintext data packet is encrypted with a second cipher streams generated from a different one of the secondary keys. In another instance, a second cipher stream generated from a single secondary key is used to encrypt a plurality of plaintext data packets. A new second cipher stream generated from another one of the secondary keys is then used for encryption following each instance of the loss of a ciphertext data packet. The index is communicated with the ciphertext to identify which secondary key is to be used in generating the second cipher stream needed for decryption. With knowledge of the secondary key to be used, re-synchronization (along with new private key negotiation) at each instance of a ciphertext data packet loss is obviated.

20 Claims, 5 Drawing Sheets



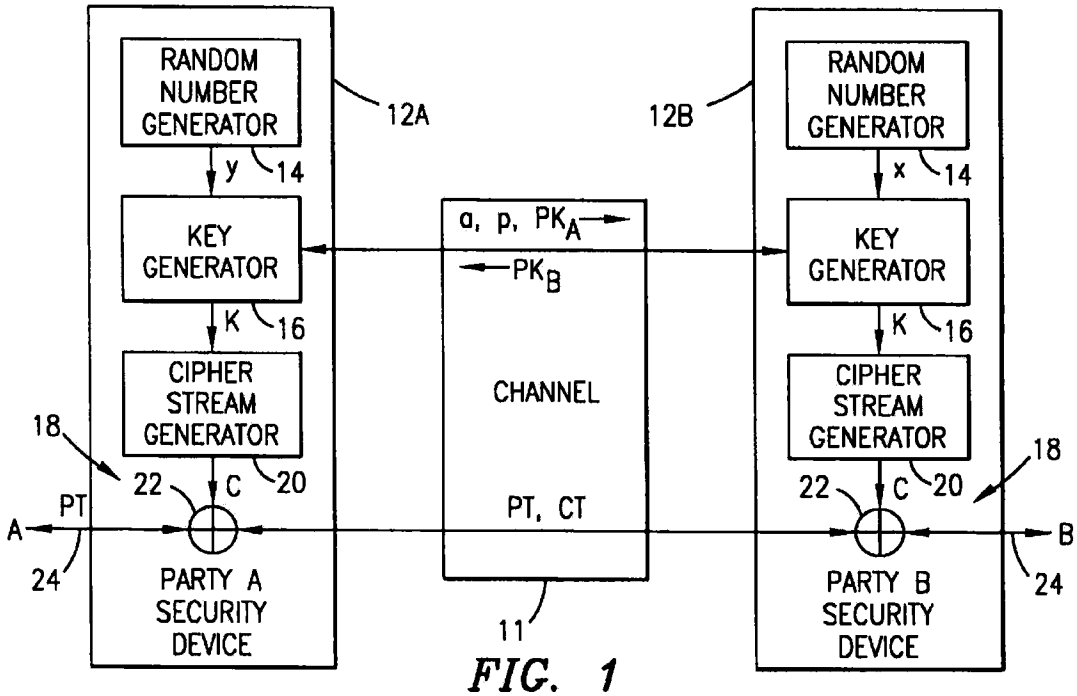


FIG. 1
(PRIOR ART)

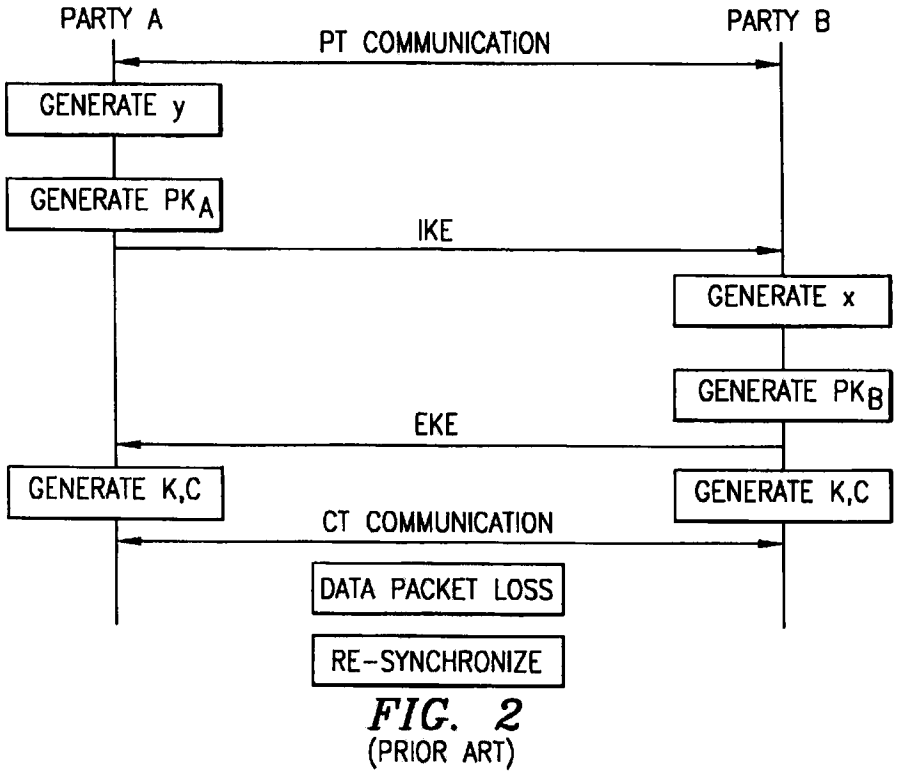


FIG. 2
(PRIOR ART)

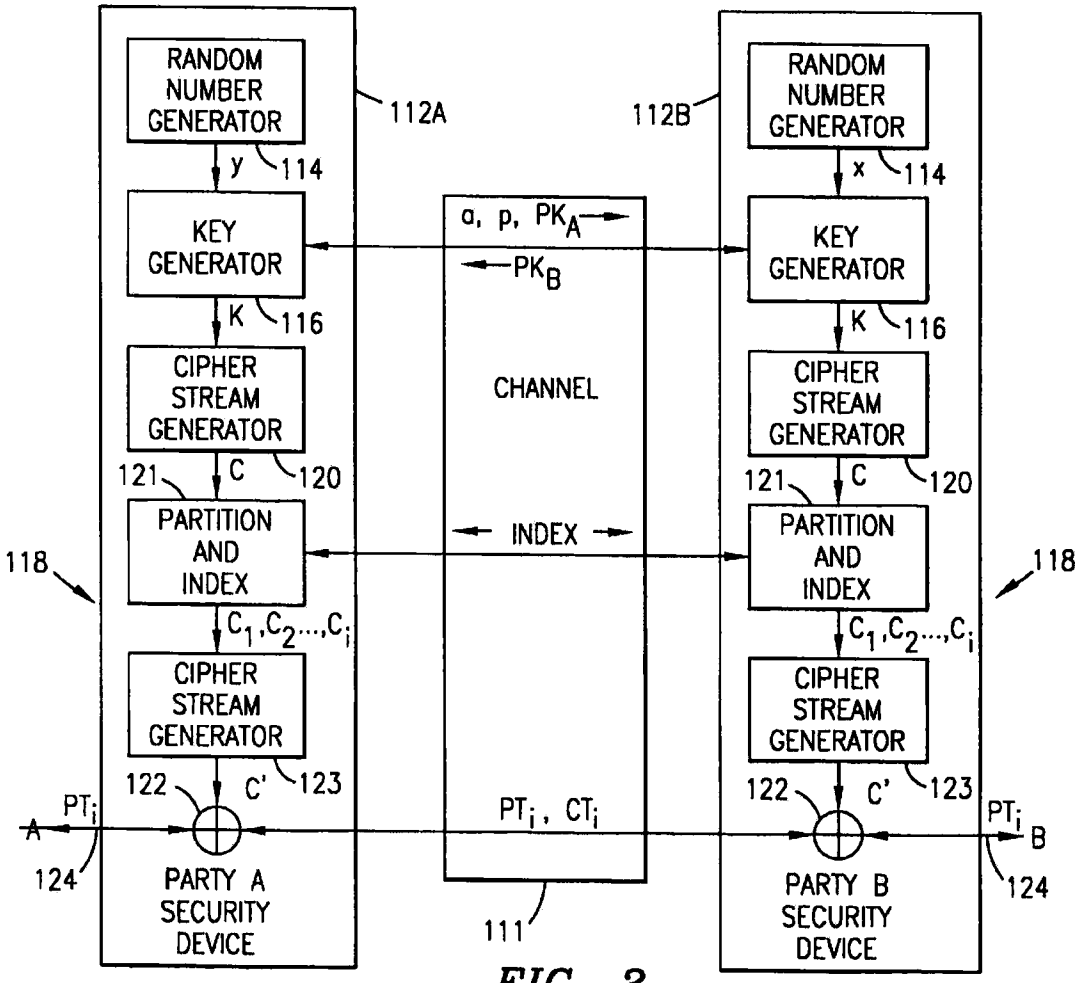

RANDOM NUMBER GENERATOR
112A
112B
y
114
x
KEY GENERATOR
K
116
CIPHER STREAM GENERATOR
C
120
121
PARTITION AND INDEX
118
$C_1, C_2 \ldots, C_i$
CIPHER STREAM GENERATOR
C'
123
122
PT_i
A
B
124
PARTY A SECURITY DEVICE
PARTY B SECURITY DEVICE
a, p, PK_A
PK_B
CHANNEL
INDEX
PT_i, CT_i
111

FIG. 3

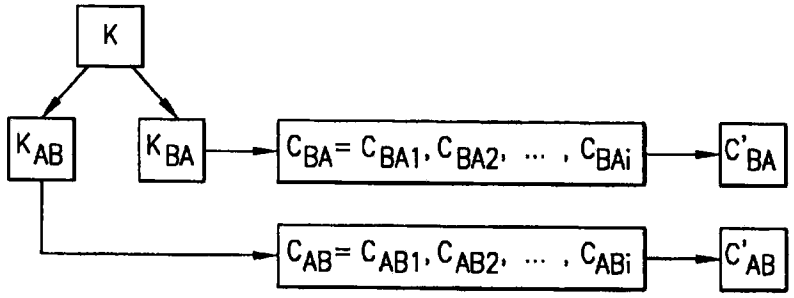

K
K_{AB}
K_{BA}
$C_{BA} = C_{BA1}, C_{BA2}, \ldots, C_{BAi}$
C'_{BA}
$C_{AB} = C_{AB1}, C_{AB2}, \ldots, C_{ABi}$
C'_{AB}

FIG. 4

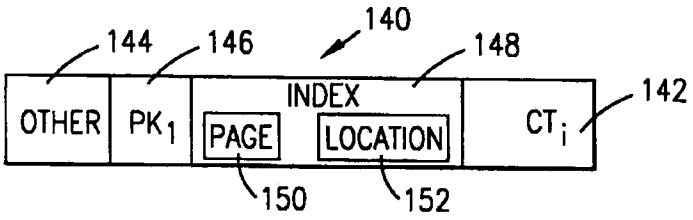


FIG. 5

C_1 C_2 C_3 . . . C_m	1 2 3 INDEX m . . (Field 152) . m	1 PAGE n (Field 150)
C_{m+1} . . . C_{2m}	1 m	2
. . .	. . .	. . .
. . . . C_i	1 . . . m	n

FIG. 6

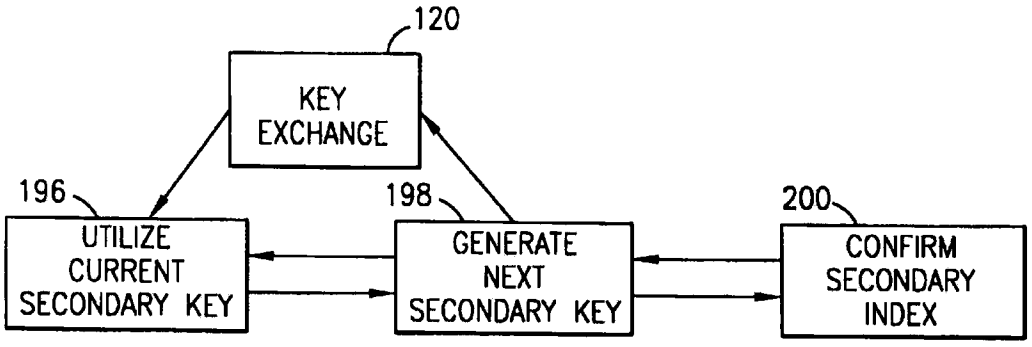


FIG. 8

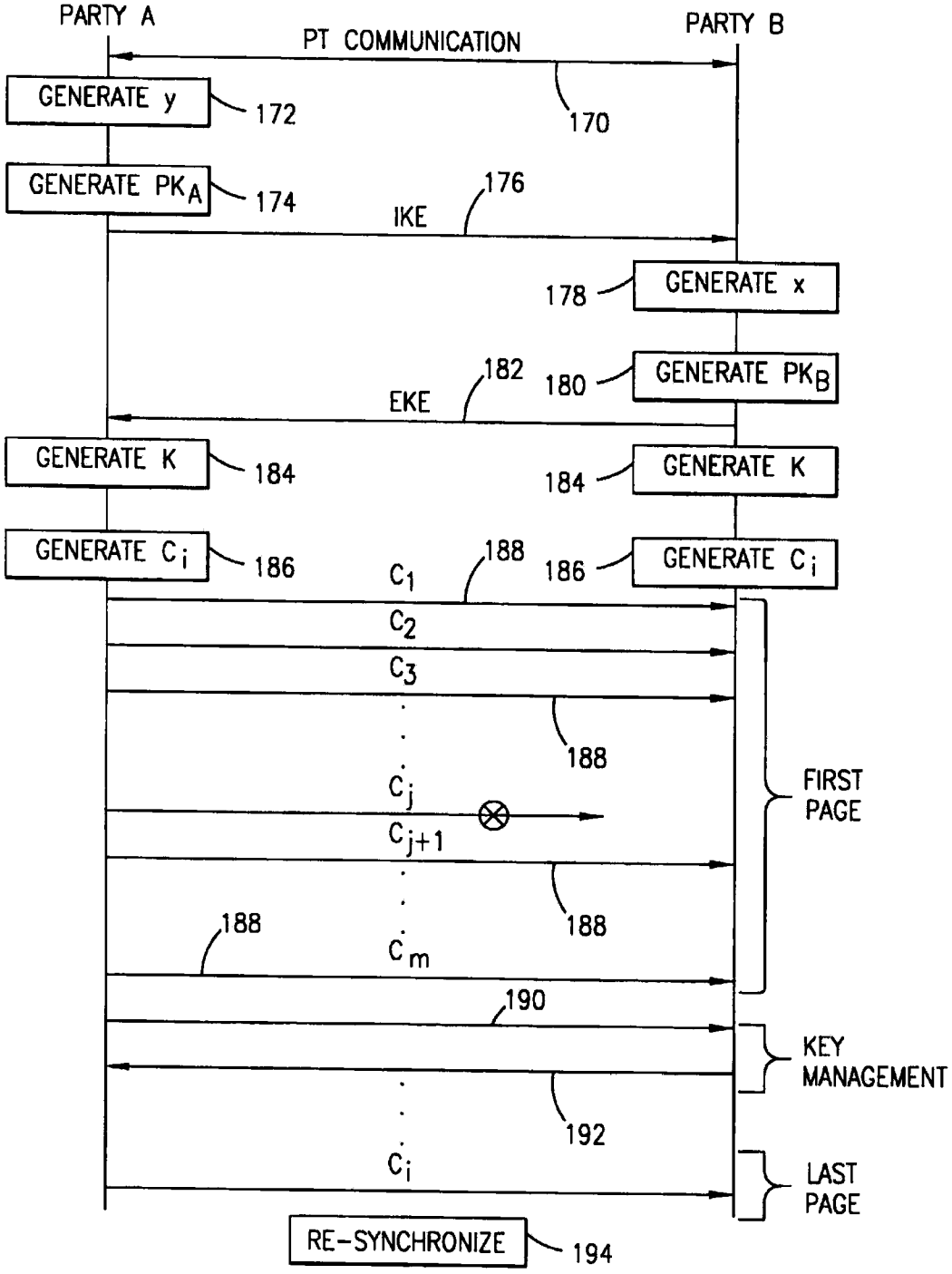

PARTY A
PT COMMUNICATION
PARTY B
GENERATE y
172
170
GENERATE PK$_A$
174
176
IKE
178
GENERATE x
182
180
GENERATE PK$_B$
EKE
GENERATE K
184
184
GENERATE K
GENERATE C$_i$
186
C$_1$
188
186
GENERATE C$_i$
C$_2$
C$_3$
188
C$_j$
C$_{j+1}$
188
188
C$_m$
190
KEY MANAGEMENT
192
C$_i$
LAST PAGE
FIRST PAGE
RE-SYNCHRONIZE
194

FIG. 7

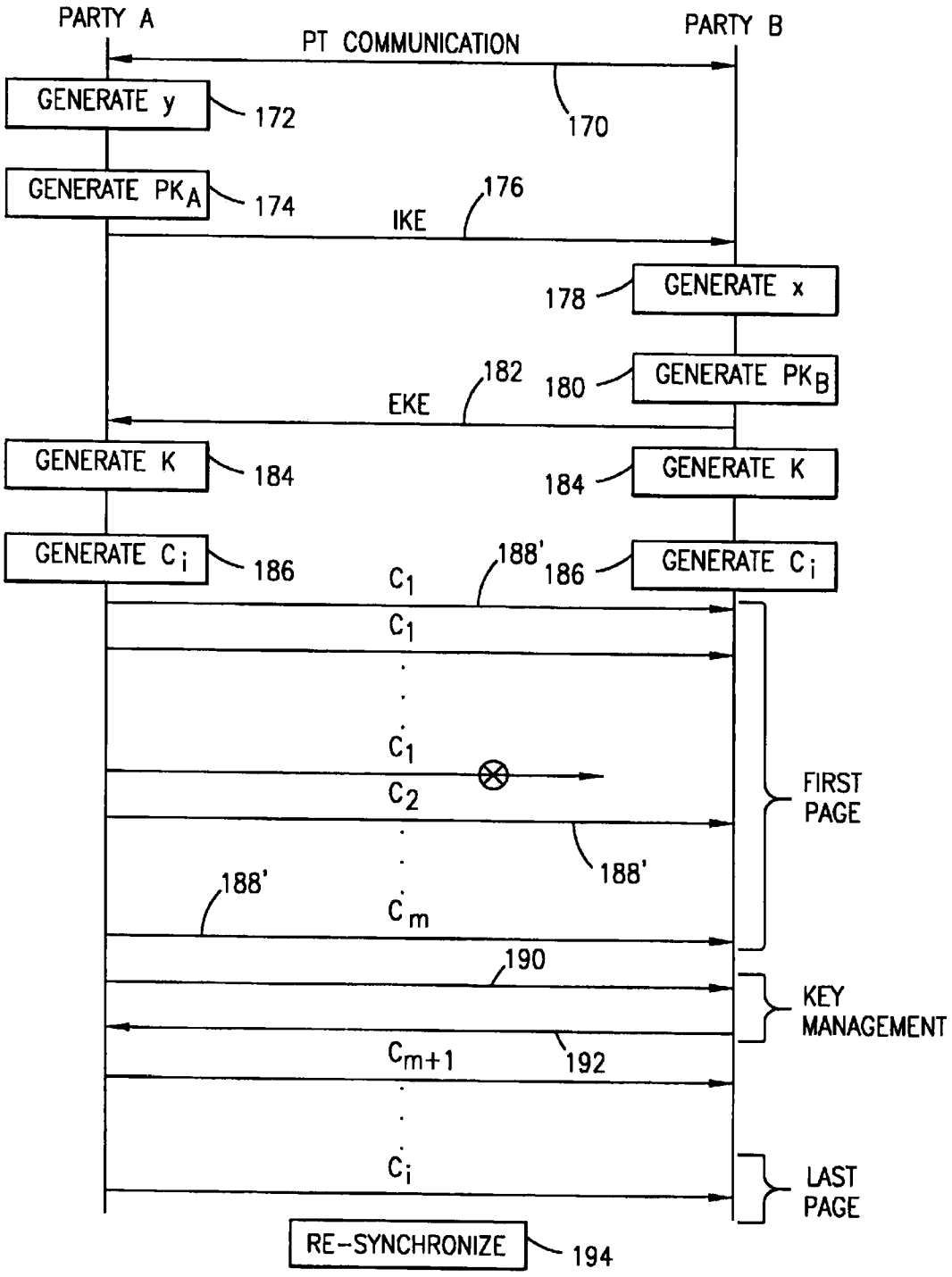

PARTY A
PT COMMUNICATION
PARTY B
GENERATE y
172
170
GENERATE PK$_A$
174
176
IKE
178
GENERATE x
182
180
GENERATE PK$_B$
EKE
GENERATE K
184
184
GENERATE K
GENERATE C$_i$
186
188'
186
GENERATE C$_i$
C$_1$
C$_1$
C$_1$
C$_2$
188'
188'
C$_m$
190
FIRST PAGE
KEY MANAGEMENT
C$_{m+1}$
192
C$_i$
LAST PAGE
RE-SYNCHRONIZE
194

FIG. 9

ENCRYPTION OF DATA PACKETS USING A SEQUENCE OF PRIVATE KEYS GENERATED FROM A PUBLIC KEY EXCHANGE

BACKGROUND OF THE INVENTION

1. Technical Field of the Invention

The present invention relates to communications and, in particular, to encrypting communications for transmission over unsecured communications channels using public key/private key techniques.

2. Description of Related Art

Communications take place over many different types of channel media such as wireline, radio frequency, fiber optic, and the like. The communications carried over each of these media are, however, subject to interception (commonly referred to as "eavesdropping"). In instances where a communication concerns sensitive or proprietary information, it is common for the parties to the communication to employ a security protocol (such as encryption or scrambling) in order to prevent the eavesdropper from being able to discover the communicated information.

In encryption, a plaintext message is encrypted by a sender into a ciphertext message using a key (cryptovariable) and then sent over a communications channel. A receiver then decrypts the communications channel transmitted ciphertext message using the same key. An eavesdropper, who presumably does not have access to the key, cannot decrypt the transmitted ciphertext message to recover the plaintext message. Any sensitive or proprietary information contained within the plaintext message is thus safely communicated.

It is not unusual for the sender and receiver to be located at a considerable distance from each other. In such cases, a number of problems arise in ensuring that the designated key necessary for decryption is securely communicated to the receiver. A secure channel, such as a courier service, may be used to communicate the key. However, such channels tend to be expensive, slow, and perhaps even unsecured in instances where the trustworthiness of the courier is compromised.

To address this problem of key distribution, public key methods have been developed for security protocols wherein a sender and receiver may independently determine a common secret key by exchanging information based on secret parameters known only to them. The information that is exchanged is known as "public keys", and although subject to intervention the common secret key cannot be determined by the eavesdropper without having access to the secret parameters. One such well known public key encryption scheme is the Diffie-Hellman algorithm. See, U.S. Pat. No. 4,200,770, to Hellman, et al. and U.S. Pat. No. 4,218,582, to Hellman, et al.

Reference is now made to FIGS. **1** and **2** wherein FIG. **1** is a block diagram of a secure communications system **10** in accordance with the prior art which implements the Diffie-Hellman public key encryption technique, and FIG. **2** is a signal flow diagram illustrating prior art key exchange, encrypted data communication, and re-synchronization processes. There are two parties, Party A and Party B, to a conversation which is being carried over an unsecured communications channel **11** supported by, for example, a wireline, radio frequency, fiber optic, or the like, communications link. Each party has access to a security device **12** positioned at opposite ends of the communications channel

11. Each security device includes a random number generator **14**, a key generator **16** and an encryption/decryption device **18** (implementing a stream cipher such as RC4). The encrypting/decrypting device **18** comprises a cipher stream generator **20** and an exclusive OR (XOR) multiplier **22**.

A data communication (perhaps comprising digitized speech or data in the form of data packets) referred to as plaintext (PT) is being carried between Party A and Party B on lines **24** and over the channel **11**. At this point in time, plaintext is being passed directly (i.e., without encryption) through the encrypting/decrypting device **18**. It is then decided to encrypt the communication. The random number generator **14** of the security device **12A** for Party A produces a secret random quantity y. Key generator **16** then generates two public quantities:

a, referred to as a base vector, which is an integer; and

p, referred to as a modulus, which is a prime number larger than a.

From these public quantities and the secret random quantity, the key generator **16** for Party A generates a public key PK_A in accordance with the following:

$$PK_A=a^Y \bmod p \tag{1}$$

The security device **12A** then initiates a key exchange with the security device **12B** for Party B. A triplet (a,p,PK_A) is sent by the security device **12A** to the security device **12B** over the communications channel **11** in a key exchange message (IKE). It will be understood that to the extent a and p are previously agreed upon by Party A and Party B, they do not need to be included in the key exchange message. It will be noted here that the key exchange message is being sent without encryption. However, this is of no concern as the function for computing PK_A is a one-way function (i.e., it is mathematically impossible for an eavesdropper to determine the secret random quantity y from knowledge of PK_A).

In response to the key exchange message, the security device **12B** for Party B has its random number generator **14** produce a secret random quantity x. Key generator **16** then generates for Party B a public key PK_B in accordance with the following:

$$PK_B=a^x \bmod p \tag{2}$$

The security device **12B** then completes the key exchange with the security device **12A** for Party A. The public key (PK_B) is sent by the security device **12B** to the security device **12A** over the communications channel **11** in a key exchange response message (EKE). It will be noted again that the key exchange response message is being sent without encryption. Again, this is of no concern as the function for computing PK_B is a one-way function, and thus the eavesdropper cannot utilize mathematical processing to determine the secret random quantity x from knowledge of PK_B.

The key generators **16** of the security devices **12** for Party A and Party B now independently generate a shared private key K in accordance with the following:

$$K=a^{xy} \bmod p \tag{3}$$

The key generator **16** for the Party A security device **12A** generates K as follows:

$$K=a^{xy} \bmod p=PK_B a^y \bmod p \tag{4}$$

Similarly, the key generator **16** for the Party B security device **12B** generates K as follows:

$$K=a^{xy} \bmod p=PK_A a^x \bmod p \quad (5)$$

While the security devices **12A** and **12B** are able to independently generate the same secret key K, it will be recognized that an eavesdropper is unable to compute the private key, in spite of having access to the public keys PK_A and PK_B, because knowledge of the necessary secret random quantities x and y is unknown and cannot be mathematically determined. The private keys K are then applied to initialize the cipher stream generators **20** which output a cipher stream C that is either exclusively ORed **22** with the plaintext (PT) to generate ciphertext (CT) for transmission over the channel **11**, or exclusively ORed with received ciphertext to generate the original plaintext.

For a bi-directional data communication between Party A and Party B as illustrated in FIG. **1**, the secret key K actually comprises (i.e., may be split into) two keys K_{AB} and K_{BA}. The first private key K_{AB} is used by security device **12A** to generate a cipher stream for encrypting Party A data communications, and by security device **12B** to generate a cipher stream for decrypting Party A data communications. Conversely, the second private key K_{BA} is used by security device **12B** to generate a cipher stream for encrypting Party B data communications, and by security device **12A** to generate a cipher stream for decrypting Party B data communications. The need for two private keys when handling bi-directional communications is required to ensure that the same generated cipher stream is never used for the encryption of different plaintext sequences.

Once the cipher stream generators **20** are initialized with the appropriate private key K, they must remain synchronized in order to ensure proper conversion between plaintext and ciphertext. The communications channel accordingly must be able to guarantee an ordered (i.e., correctly sequenced) delivery of any encrypted sequenced data packets so that synchronization may be maintained. In the event synchronization is lost, for example due to a loss of an encrypted data packet during transmission over the channel **11**, re-synchronization followed by encryption with a new private key must occur. This is so because the recovery of plaintext is easily accomplished with knowledge of two different plaintext messages encrypted with the same cipher stream C (i.e., produced from the same private key K).

Re-synchronization then requires a new exchange of public keys, followed by the independent generation of another private key and appropriate initialization of the cipher stream generators **20**. This process is undesirable as it significantly delays completion of the data communication and consumes valuable communications resources (i.e., wastes bandwidth) on the channel **11** during the key exchange that could otherwise be used in carrying communications which generate revenue. Furthermore, if one of the parties to the communication comprises a mobile communications device (such as a cellular telephone) the computation of the private key is a processor intensive operation requiring a significant time expenditure and causing a significant drain on battery power resources.

The incidence of encrypted data packet loss necessitating re-synchronization is especially high in connection with those communications channels **11**, such as wireless radio frequency communications channels, which suffer from interference, distortion or fading. In fact, a five to ten percent data packet loss rate in connection with the use of wireless communications channels is not uncommon. Each instance of packet loss in connection with encrypted sensitive or proprietary information data communications then unfortunately necessitates an inefficient re-synchronization. For sensitive or proprietary information data communications carried over such communications channels, there is a need then for a more efficient and effective security protocol which does not necessarily require re-synchronization in the event of a data packet loss.

SUMMARY OF THE INVENTION

To obviate the need for re-synchronization following loss of a ciphertext data packet, the present invention partitions a private key generated cipher stream into an indexed sequence of secondary keys. The secondary keys are then utilized on a selective basis to encrypt plaintext data packets for transmission over a communications channel. Each transmitted ciphertext data packet then includes an index identifying which of the plurality of secondary keys was used for the encryption. In one embodiment, each plaintext data packet is encrypted by a cipher stream generated from a different one of the secondary keys. In another embodiment, the a cipher stream generated from a single secondary key is utilized to encrypt plaintext data packets until loss of a ciphertext data packet occurs. At that point, a cipher stream generated from a next one of the plurality of secondary keys is used for encryption. In each case, however, no re-synchronization need occur as the index included with each ciphertext data packet identifies the secondary key to be used for decryption.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the method and apparatus of the present invention may be acquired by reference to the following Detailed Description when taken in conjunction with the accompanying Drawings wherein:

FIG. **1** (previously described) is a block diagram of a secure communications system in accordance with the prior art which implements the Diffie-Hellman public key encryption technique;

FIG. **2** (previously described) is a signal flow diagram illustrating prior art key exchange, encrypted data communication, and re-synchronization processes;

FIG. **3** is a block diagram of a secure communications system in accordance with the present invention;

FIG. **4** is a flow diagram for secondary private key generation;

FIG. **5** is a simplified format used for the transmission of an encrypted data communication in accordance with the present invention;

FIG. **6** is a diagram illustrating a page organization of the sequence of secondary private keys;

FIG. **7** is a signal flow diagram illustrating the key exchange, encrypted data communication, and re-synchronization processes of the present invention;

FIG. **8** is a state control diagram illustrating an encryption key management process of the present invention; and

FIG. **9** is a signal flow diagram illustrating the key exchange, encrypted data communication, and re-synchronization processes of an alternative embodiment for the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

Reference is now made to FIG. **3** wherein there is shown a block diagram of a secure communications system **100** in accordance with the present invention. There are two parties,

Party A and Party B, to a conversation which is being carried over an unsecured communications channel **111** supported by, for example, a wireline, radio frequency, fiber optic, or the like, communications link. Each party has access to a security device **112** positioned at opposite ends of the communications channel **111**. Each security device includes a random number generator **114**, a key generator **116** and an encrypting/decrypting device **118** (implementing any suitable stream cipher including, for example, RC4). The encrypting/decrypting device **118** comprises a first cipher stream generator **120**, a partitioning and indexing device **121**, a second cipher stream generator **123** and an exclusive OR (XOR) multiplier **122**.

A data communication (perhaps comprising digitized speech or data in the form of data packets) referred to as plaintext (PT) is being carried between Party A and Party B on lines **124** and over the channel **111**. At this point in time, plaintext is being passed directly (i.e., without encryption) through the encrypting/decrypting device **118**. A decision is then made to switch to encrypted communication. The selection of a common secret key for encrypting Party A and Party B communications may be made using any suitable public key exchange method including, for example, the Diffie-Hellman method. The random number generator **114** of the security device **112**A for Party A produces a random quantity y. Key generator **116** then generates the two public quantities a and p. From these public quantities and the secret random quantity, the key generator **114** for Party A generates a public key PK_A in accordance with Equation (1). The security device **112**A then initiates a key exchange with the security device **112**B for Party B. A triplet (a,p,PK_A) is sent by the security device **112**A to the security device **112**B over the communications channel **111** in a key exchange message (IKE). It will be understood that to the extent a and p are previously agreed upon by Party A and Party B, they do not need to be included in the key exchange message. It will be remembered that the key exchange message is being sent without encryption. However, this is of no concern as the function for computing PK_A is a one-way function (i.e., it is mathematically impossible for an eavesdropper to determine the secret random quantity y from knowledge of PK_A) .

In response to the key exchange message, the security device **112**B for Party B has its random number generator **114** produce a random quantity x. Key generator **116** then generates for Party B a public key PK_B in accordance with Equation (2). The security device **112**B then completes the key exchange with the security device **112**A for Party A. The public key (PK_B) is sent by the security device **112**B to the security device **112**A over the communications channel **111** in a key exchange response message (EKE). It will be remembered that the key exchange response message is being sent without encryption. Again, this is of no concern as the function for computing PK_B is a one-way function, and thus the eavesdropper cannot utilize mathematical processing to determine the secret random quantity x from knowledge of PK_B.

The key generators **116** of the security devices **112** for Party A and Party B now independently generate a shared private key K in accordance with Equations (4) and (5), respectively. While the security devices **112**A and **112**B are able to independently generate the same private key K, it will be recognized that an eavesdropper is unable to compute the private key, in spite of having access to the public keys PK_A and PK_B, because knowledge of the secret random quantities x and y is unknown and cannot be mathematically determined. The private keys K are then applied to initialize the first cipher stream generators **120** which output a first cipher stream C.

This first cipher stream C is then processed by the partition and index device **121** which partitions the cipher stream into a sequence of secondary private keys C_1, C_2, . . . , C_i. The sequence of secondary private keys C_1, C_2, . . . , C_i is then applied to initialize the second cipher stream generators **123** which output a second cipher stream C'. This second cipher stream C' is then either exclusively ORed **122** with the plaintext sequence (PT_i) to generate ciphertext (CT_i) for transmission over the channel **111**, or exclusively ORed with received ciphertext to generate plaintext. Each secondary private key C_i is further provisioned by the device **121** with a uniquely identifying index. The index indicating which secondary private key C_i is being used to encrypt a particular plaintext sequence PT_i is communicated over the channel **111** to ensure synchronization and the utilization of the correct key for decryption. This index may be exchanged between the security devices **112** in un-encrypted form because it bears no information concerning the secondary private key C_i other than a sequence (i.e., indexing) number.

Reference is now made to FIG. **4** wherein there is shown a flow diagram for secondary private key generation. For a bi-directional data communication between Party A and Party B as illustrated in FIG. **3**, the private key K actually comprises (i.e., may be split into) two keys K_{AB} and K_{BA}. The need for two private keys when handling bi-directional communications is required to ensure that the same cipher stream is never used for the encryption of different plaintext sequences. The first private key K_{AB} is used to generate a forward first cipher stream C_{AB}, and the second private key K_{BA} is used to generate a reverse first cipher stream C_{BA}. The forward first cipher stream C_{AB} is then partitioned and indexed to generate a first (or forward channel) secondary private key C_{ABi} sequence, with individual ones in the sequence used to generate a forward second cipher stream C_{AB}' that is used by security device **112**A to encrypt Party A PT_i data communications, and by security device **112**B to decrypt Party A CT_i data communications. The reverse first cipher stream C_{BA}, on the other hand, is then partitioned and indexed to generate a second (or reverse channel) secondary private key C_{BAi} sequence, with individual ones in the sequence used to generate a reverse second cipher stream C_{BA}' that is used by security device **112**B to encrypt Party B PT_i data communications, and by security device **112**A to decrypt Party B CT_i data communications.

Reference is now made to FIG. **5** wherein there is shown a simplified format **140** used for the transmission of an encrypted data communication segment (CT_i) **142** in accordance with the present invention. The format **140** includes a plurality of fields (OTHER) **144** relating, for example, to packet reconstruction, compression and network layer protocol, which are not relevant to the present invention. The format further includes a primary key index field (PKI) **146** which indicates the parity of the primary encryption/decryption key K used to generate the plurality of secondary keys C_i. A secondary key index field **148**, comprising a page identification **150** and a location (on the page) identification **152**, is also included in the format **140**. As noted above, a sequence of secondary private keys C_1, C_2, . . . , C_i is generated. The i generated keys are arranged in n groups (or pages) of m keys each. The page identification **152** accordingly identifies which of the n groups of keys is being used to encrypt the data. The location identification **152** then identifies which particular one of the m keys on the identified page n is being used to encrypt the data. This page organization of the sequence of secondary private keys C_1, C_2, . . . , C_i is illustrated in FIG. **6**.

Reference is now made to FIG. 7 wherein there is shown a signal flow diagram illustrating the key exchange, encrypted data communication, and re-synchronization processes of the present invention. Party A and Party B are engaged in a plaintext communication **170**. The public key exchange process is then initiated with Party A generation of the secret quantity y (action **172**) and the public key PK_A (action **174**). The key exchange message (IKE) **176** is then sent to Party B. Party B responds by generating secret quantity x (action **178**) and the public key PK_B (action **180**). The key exchange response message (EKE) **182** is then sent to Party A. Party A and Party B then independently generate (action **184**) the private key K from which the sequence of secondary private keys $C_1, C_2, \ldots, C_i$ is generated (action **186**).

In order to simplify the illustration, only the encryption of data communications **188** transmitted from Party A to Party B is shown. A first plaintext sequence PT_1 is then encrypted using a second cipher stream C' generated from the first one of the secondary private keys C_1 to produce a first ciphertext sequence CT_1. A similar process is used to produce a second ciphertext sequence CT_2 from a second cipher stream C' generated from the second one of the secondary private keys C_2. This process continues for each of the subsequent plaintext sequences PT_i.

It is noted, however, that with respect to the j-th plaintext sequence PT_j encrypted with a second cipher stream C' generated from the secondary private key C_j, the ciphertext sequence CT_j was not successfully transmitted (as indicated by "X"). In accordance with the prior art process as illustrated in FIG. **2**, this packet loss would require an immediate re-synchronization necessitating a new public key exchange and cipher stream initialization. In the present invention, synchronization is maintained allowing for continued packet transmission starting with the ciphertext sequence CT_{j+1} encrypted using a second cipher stream C' generated from the secondary private key C_{j+1}. The reason synchronization is maintained is that each ciphertext sequence CT_i is formatted for transmission (FIG. **5**) to include information (index **148**) identifying which secondary key (page and location) should be utilized in generated the second cipher stream C' needed for decrypting the transmission. As plural keys have been negotiated and the current encryption key can be identified, there is no need to negotiate a new key for continuing with the communication.

Following the processing of one page of data packets (i.e., the encryption of m plaintext sequences PT_i with individual second cipher streams C' generated from m secondary private keys C_i), a key management message **190** is sent from Party A to Party B. This message **190** identifies the index m and page n that Party A is using to encrypt (and/or decrypt) data communications. Responsive to the message **190**, Party B sends a key management response message **192** confirming its coordinated use of a secondary private key from the same page n, and index m therein, for encryption and decryption. Encryption in the foregoing manner utilizing a second cipher stream C' generated from an appropriate next secondary secret key then ensues. Key management occurs following the use of a last secondary secret key of a page.

Then, following the processing of all pages of data packets (i.e., the encryption of i plaintext sequences PT_i, the last one being encrypted with a second cipher stream C' generated from the secondary private key C_i), the process re-synchronizes **194** to invoke the generation of a new set of secondary private keys (actions **184** and **186**). Accordingly, secret quantities must be selected (actions **172** and **178**), public keys generated (actions **174** and **180**), and key exchange messages (IKE/EKE) **176** and **182** sent.

Reference is now made to FIG. **8** wherein there is shown a state control diagram illustrating an encryption key management process of the present invention. In normal operation, the protocol state for key management transitions between a utilize current secondary private key state **196** and a generate next secondary private key state **198**. In state **196**, a data packet is either encrypted or decrypted using a second cipher stream generated from the current secondary private key. A transition is then made, following each encryption/decryption, to state **198** where a next secondary private key is generated. A transition is then made back to state **196** where this newly generate secondary private key becomes the current one for use in generating the second cipher stream needed for encrypting or decrypting a next data packet.

Maintenance of synchronization between Party A and Party B as to the proper secondary private key is accomplished through either a passive operation, an active secondary key operation, or an active primary key operation. In passive operation, no message exchange between Party A and Party B regarding synchronization is required as the index is merely passively incremented with each encryption or decryption and monitoring of the index field **148** (FIG. **5**) of each sent ciphertext sequence CT_i.

In active secondary key operation, a transition is made from state **198** to a confirm secondary index state **200**. In the state **198**, key management messages **190** and **192** (FIG. **7**) are exchanged between Party A and Party B confirming coordinated use of a secondary private key from the same page n, and index m therein, for encryption and decryption. Once secondary key confirmation has been received, a transition is made back to state **198**. With respect to the page organization of secondary private keys C_i illustrated in FIG. **6**, state **200** is entered into following the completed transmission of one page worth of data packets.

In active primary key operation, a transition is made from state **198** to a key exchange state **202**. In state **202**, a re-synchronization is performed to invoke the generation of a new set of secondary private keys (actions **184** and **186** of FIG. **7**) by selecting new secret quantities, generating new public keys generated and sending key exchange messages (IKE/EKE). With respect to the page organization of secondary private keys C_i illustrated in FIG. **6**, state **202** is entered into following the completed transmission of all n pages worth of data packets.

Simplified pseudo code describing state transitions in FIG. **8** with respect to passive secondary key operation may be written as follows:

```
IF request for next secondary private key
THEN increment index
IF index<=m
THEN {use secondary key at incremented index location}
IF index>m AND page<n
THEN initiate active secondary key operation
ELSE {full sequence of secondary private keys Ci used,
  initiate active primary key operation}
```

Simplified pseudo code describing state transitions in FIG. **8** with respect to encrypting side active secondary key operation may be written as follows:

```
IF secondary key requested>m
THEN reset index
IF page<=n
THEN {send key management message to peer
  (decrypting entity) identifying next page}
```

IF peer responds and confirms
THEN {increment page, use first secondary private key at incremented page location}
ELSE IF {error regarding key management message}
THEN repeat procedure
ELSE {full sequence of secondary private keys C_i and secondary key pages used, initiate active primary key operation}

Simplified pseudo code describing state transitions in FIG. **8** with respect to decrypting side active secondary key operation may be written as follows:

IF {key management message received from peer (encrypting entity) identifies page greater than current page}
THEN {increment page to match identified page respond to key management message
IF {data packet received with page index set to incremented page}
THEN {initialize decryption using secondary key indexed from incremented page}
}

Simplified pseudo code describing state transitions in FIG. **8** with respect to Party A active primary key operation may be written as follows:

IF new primary keys are required
THEN construct and send IKE message (plaintext)
IF {receive EKE message responsive to IKE message}
THEN {execute public key algorithms, deduce new private key and secondary private keys}
ELSE IF error regarding IKE message
THEN complete procedure or retransmit IKE
IF receive an EKE message (response required)
THEN discard EKE message
IF receive an EKE message (response required)
THEN construct and transmit an IKE message (plaintext)

Simplified pseudo code describing state transitions in FIG. **8** with respect to Party B active primary key operation may be written as follows:

IF new primary keys are required
THEN construct and send EKE message (plaintext)
IF receive IKE message
THEN {execute public key algorithms, deduce new private key and secondary private keys}
IF receive IKE message (response required)
THEN {construct and transmit EKE message (plaintext), execute public key algorithms, deduce new private key and secondary private keys, advance index}
ELSE IF error regarding EKE message
THEN complete procedure
IF receive IKE message (response required)
THEN {construct and transmit EKE message (plaintext), execute public key algorithms, deduce new private key and secondary private keys, advance index}

Reference is now once again made to the state control diagram of FIG. **8** for a description of an alternative embodiment of the present invention. It will be remembered that in connection with the prior description, the protocol state for key management transitions between the current secondary private key state **196** and the generate next secondary private key state **198**. The transition from state **196** (data packet encryption/decryption using the current secondary private key) to state **198** (where a next secondary private key is generated) occurs after each such encryption/decryption operation on a data packet. In the current embodiment, this transition occurs only each time that a data packet delivery fails. Thus, a second cipher stream C' generated from a single secondary private key is used to encrypt/decrypt plural data packets. It is only when a packet delivery failure occurs that the index is incremented and a new secondary private key is accessed for use. As before, maintenance of synchronization between Party A and Party B as to the proper secondary private key for use is accomplished through either the passive operation, the active secondary key operation, or the active primary key operation.

Reference is now made to FIG. **9** wherein there is shown a signal flow diagram illustrating the key exchange, encrypted data communication, and re-synchronization processes of an alternate embodiment for the present invention. Party A and Party B are engaged in a plaintext communication **170**. The public key exchange process is then initiated with Party A generation of the secret quantity y (action **172**) and the public key PK_A (action **174**). The key exchange message (IKE) **176** is then sent to Party B. Party B responds by generating secret quantity x (action **178**) and the public key PK_B (action **180**). The key exchange response message (EKE) **182** is then sent to Party A. Party A and Party B then independently generate (action **184**) the private key K from which the sequence of secondary private keys $C_1, C_2, \ldots, C_i$ is generated (action **186**).

In order to simplify the illustration, only the encryption of data communications **188'** transmitted from Party A to Party B is shown. A first one of the secondary private keys C_1 is used to generate a second cipher stream C' for encrypting plural plaintext sequences PT and producing corresponding ciphertext sequences CT. The use of the second cipher stream C' generated from a single secondary private key C_1 to encrypt plaintext sequences continues until such time as a delivery failure occurs (as indicated by "X"). At that point, a next one of the secondary private keys C_2 is used to generate a new second cipher stream C' for encrypting subsequent plural plaintext sequences PT and producing corresponding ciphertext sequences CT. Again, as in the prior embodiment, the reason synchronization is maintained in spite of delivery failure is that each ciphertext sequence CT is formatted for transmission (FIG. **5**) to include information (index **148**) identifying which secondary key should be utilized to generate the second cipher stream C' needed for decrypting the transmission. As the encryption key can be identified, there is no need to negotiate a new key for continuing with the communication.

Following the use one page worth (i.e., m in number) of secondary private keys C_i to generate corresponding second cipher streams C' each encrypting a plurality of plaintext sequences PT, a key management message **190** is sent from Party A to Party B. This message **190** identifies the index m and page n that Party A is using to encrypt (and/or decrypt) data communications. Responsive to the message **190**, Party B sends a key management response message **192** confirming its coordinated use of a secondary private key from the same page n, and index m therein, for encryption and decryption. Encryption in the foregoing manner utilizing a second cipher stream C' generated from an appropriate next secondary secret key then ensues. Key management occurs following the use of a last secondary secret key of a page. Then, following the use of all pages (i.e., n in number) of secondary private keys C_i to generate second cipher streams C' for encrypting a plurality of plaintext sequences PT (the last sequence of data packets being encrypted with a second cipher stream generated from the secondary private key C_i), the process re-synchronizes **194** to invoke the generation of a new set of secondary private keys (actions **184** and **186**). Accordingly, secret quantities must be selected (actions **172**

and 178), public keys generated (actions 174 and 180), and key exchange messages (IKE/EKE) 176 and 182 are sent.

The pseudo code previously provided is equally applicable to this embodiment, with minor modification as necessary to account for the operational difference between utilizing a new key with each sequence/packet and using a new key with each delivery failure.

It will be recognized that this embodiment of the present invention utilizes secondary private keys at a much lower rate than the preceding embodiment. Thus, key management transactions (190 and 192) as well as re-synchronization actions (194) occur less frequently, and a more efficient use of limited bandwidth communications resources is made.

Although preferred embodiments of the method and apparatus of the present invention have been illustrated in the accompanying Drawings and described in the foregoing Detailed Description, it will be understood that the invention is not limited to the embodiments disclosed, but is capable of numerous rearrangements, modifications and substitutions without departing from the spirit of the invention as set forth and defined by the following claims.

What is claimed is:

1. A private key generator, comprising:

a first generator for generating a private key;

a second generator initialized with the private key for generating a first cipher stream;

a partitioner that partitions the first cipher stream into a plurality of secondary keys for use in generating corresponding second cipher streams to encrypt plaintext information into ciphertext information; and

an indexer for indexing the plurality of secondary keys, an index included with the ciphertext information identifying which of the indexed plurality of secondary keys was used in encrypting the plaintext information.

2. The private key generator as in claim 1 further including:

means for exchanging public keys; and

wherein the first generator functions to generate the private key from processing at least one of the exchanged public keys.

3. The private key generator as in claim 1 wherein the plaintext information comprises a plurality of plaintext packets, each plaintext packet encrypted with a second cipher stream generated from a different one of the secondary keys.

4. The private key generator as in claim 1 wherein the plaintext information comprises a plurality of plaintext packets, each sequence of plaintext packets handled between instances of ciphertext information loss encrypted with a second cipher stream generated from a different one of the secondary keys.

5. The private key generator as in claim 1 wherein the first generator generates a new private key when each of the generated plurality of secondary keys from a prior private key has been used for encryption.

6. A method for generating a private key, comprising the steps of:

generating a private key;

generating a first cipher stream initialized from the generated private key;

partitioning the first cipher stream into a plurality of secondary keys for use in generating corresponding second cipher streams to encrypt plaintext information into ciphertext information; and

indexing the plurality of secondary keys, an index included with the ciphertext information identifying which of the indexed plurality of secondary keys was used in encrypting the plaintext information.

7. The method as in claim 6 further including the steps of:

exchanging public keys; and

generating the private key from processing at least one of the exchanged public keys.

8. The method as in claim 6 wherein the plaintext information comprises a plurality of plaintext packets, further including the steps of:

generating a plurality of second cipher streams, each second cipher stream initialized from a different one of the secondary keys; and

encrypting each plaintext packet with a different one of the plurality of second cipher streams.

9. The method as in claim 6 wherein the plaintext information comprises a plurality of plaintext packets, further including the steps of:

generating a plurality of second cipher streams, each second cipher stream initialized from a different one of the secondary keys; and

encrypting each sequence of plaintext packets handled between instances of ciphertext information loss with a different one of the plurality of second cipher streams.

10. The method as in claim 6 further including the step of repeating the steps of claim 6 when each of the generated plurality of secondary keys has been used for encryption.

11. An encryption device, comprising:

a first generator for generating a private key;

a second generator initialized with the private key for generating a first cipher stream;

a partitioner for partitioning the first cipher stream into a plurality of secondary keys;

an indexer for indexing the plurality of secondary keys;

means for encrypting plaintext information into ciphertext information using second cipher streams generated from the plurality of secondary keys; and

means for including an index with the ciphertext information identifying which of the indexed plurality of secondary keys was used in encrypting the plaintext information.

12. The encryption device as in claim 11 further including:

means for exchanging public keys; and

wherein the first generator functions to generate the private key from processing at least one of the exchanged public keys.

13. The encryption device as in claim 11 wherein the plaintext information comprises a plurality of plaintext packets, and wherein the means for encrypting comprises:

a third generator initialized with the secondary keys for generating corresponding second cipher streams; and

means for encrypting each plaintext packet with a different one of the second cipher streams.

14. The encryption device as in claim 11 wherein the plaintext information comprises a plurality of plaintext packets, and wherein the means for encrypting comprises:

a third generator initialized with the secondary keys for generating corresponding second cipher streams; and

means for encrypting each one of a plurality of sequences of plaintext packets that is handled between instances of ciphertext information loss with a different one of the second cipher streams.

15. The encryption device as in claim 11 wherein the first generator generates a new private key when each of the

generated plurality of secondary keys from a prior private key has been used for encryption.

16. A method for encrypting, comprising the steps of:

generating a private key;

generating a first cipher stream initialized from the generated private key;

partitioning the first cipher stream into a plurality of secondary keys;

indexing the plurality of secondary keys;

encrypting plaintext information into ciphertext information using second cipher streams generated from the plurality of secondary keys; and

including with the ciphertext information an index identifying which of the indexed plurality of secondary keys was used in encrypting the plaintext information.

17. The method as in claim 16 further including the steps of:

exchanging public keys; and

generating the private key from processing at least one of the exchanged public keys.

18. The method as in claim 16 wherein the plaintext information comprises a plurality of plaintext packets, and the step of encrypting comprises the steps of:

generating second cipher streams each initialized from a different one of the plurality of secondary keys; and

encrypting each plaintext packet with a different one of the second cipher streams.

19. The method as in claim 16 wherein the plaintext information comprises a plurality of plaintext packets, and the step of encrypting comprises the steps of:

generating second cipher streams each initialized from a different one of the plurality of secondary keys; and

encrypting each sequence of plaintext packets handled between instances of ciphertext information loss with a different one of the second cipher streams.

20. The method as in claim 16 further including the step of repeating the steps of claim 16 when each of the generated plurality of secondary keys has been used for encryption.

* * * * *

Exhibit 4

US005797134A

United States Patent [19]

McMillan et al.

[11] Patent Number: 5,797,134

[45] Date of Patent: Aug. 18, 1998

[54] **MOTOR VEHICLE MONITORING SYSTEM FOR DETERMINING A COST OF INSURANCE**

[75] Inventors: **Robert John McMillan**, Tampa, Fla.; **Alexander Dean Craig**, Moreland Hills, Ohio; **John Patrick Heinen**, Tampa, Fla.

[73] Assignee: **Progressive Casualty Insurance Company**, Mayfield Village, Ohio

[21] Appl. No.: **592,958**

[22] Filed: **Jan. 29, 1996**

[51] **Int. Cl.**[6] **G06F 17/60**

[52] **U.S. Cl.** **705/400**; 705/4

[58] **Field of Search** 395/204; 364/424.01, 364/424.04, 565; 340/441; 346/18; 705/4, 400

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,533,962	8/1985	Decker et al. .	
4,608,638	8/1986	Tsikos .	
4,667,336	5/1987	Best .	
4,763,745	8/1988	Eto et al. .	
4,807,179	2/1989	Clere et al. .	
4,829,434	5/1989	Karmel et al. .	
4,843,463	6/1989	Michetti .	
4,843,578	6/1989	Wade	364/565
4,853,720	8/1989	Onari et al. .	
4,939,652	7/1990	Steiner .	
4,987,541	1/1991	Levente et al. .	
4,992,943	2/1991	McCracken .	
5,055,851	10/1991	Sheffer	342/457
5,111,289	5/1992	Lucas et al. .	
5,189,621	2/1993	Onari et al. .	
5,223,844	6/1993	Mansell et al.	342/357
5,319,374	6/1994	Desai et al.	342/387
5,365,451	11/1994	Wang et al.	364/449
5,430,432	7/1995	Camhi et al.	340/438
5,499,182	3/1996	Ousborne	364/424.04
5,548,273	8/1996	Nicol et al.	340/439
5,550,551	8/1996	Alesio	342/457
5,638,273	6/1997	Coiner et al.	364/424.04

FOREIGN PATENT DOCUMENTS

9002388 8/1989 WIPO .

OTHER PUBLICATIONS

Rosenberg, Martin; Alexander, Shephen A. Rate Classification Reform in New Jersey, Best's Review(Prop/Casualty) vol. 92, No. 12, pp. 30–32, Apr. 1992.

Kaneko, Tetsuya; Jovanis, Paul P. Multiday driving patterns and motro carrier accident risk. A disaggregate analysis. Accident Analysis and Prevention, vol. 24, No. 5, pp. 437–456, Jan. 1, 1992.

"The Safest Cars of '91"; Baig, Edward U.S. News & World Report, v109, n22, p. 71; Dec. 3, 1990.

"Vendors Spice Up Services"; Robert Deierlein Beverage World, v109, n1467, p. 82; Jun. 1990.

Primary Examiner—Edward R. Cosimano

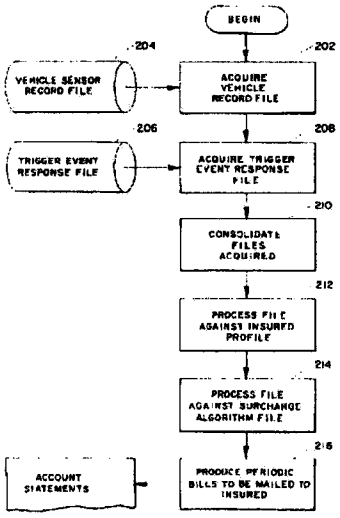
Assistant Examiner—Thanh-Hang Voqui

Attorney, Agent, or Firm—Fay, Sharpe, Beall, Fagan, Minnich and McKee

[57] **ABSTRACT**

A method and system of determining a cost of automobile insurance based upon monitoring, recording and communicating data representative of operator and vehicle driving characteristics. The cost is adjustable retrospectively and can be prospectively set by relating the driving characteristics to predetermined safety standards. The method comprises steps of monitoring a plurality of raw data elements representative of an operating state of the vehicle or an action of the operator. Selected ones of the raw data elements are recorded when the ones are determined to have an identified relationship to safety standards. The selected ones are consolidated for processing against an insurer profile and for identifying a surcharge or discount to be applied to a base cost of automobile insurance. A final cost is produced from the base costs and the surcharges or discounts.

26 Claims, 6 Drawing Sheets



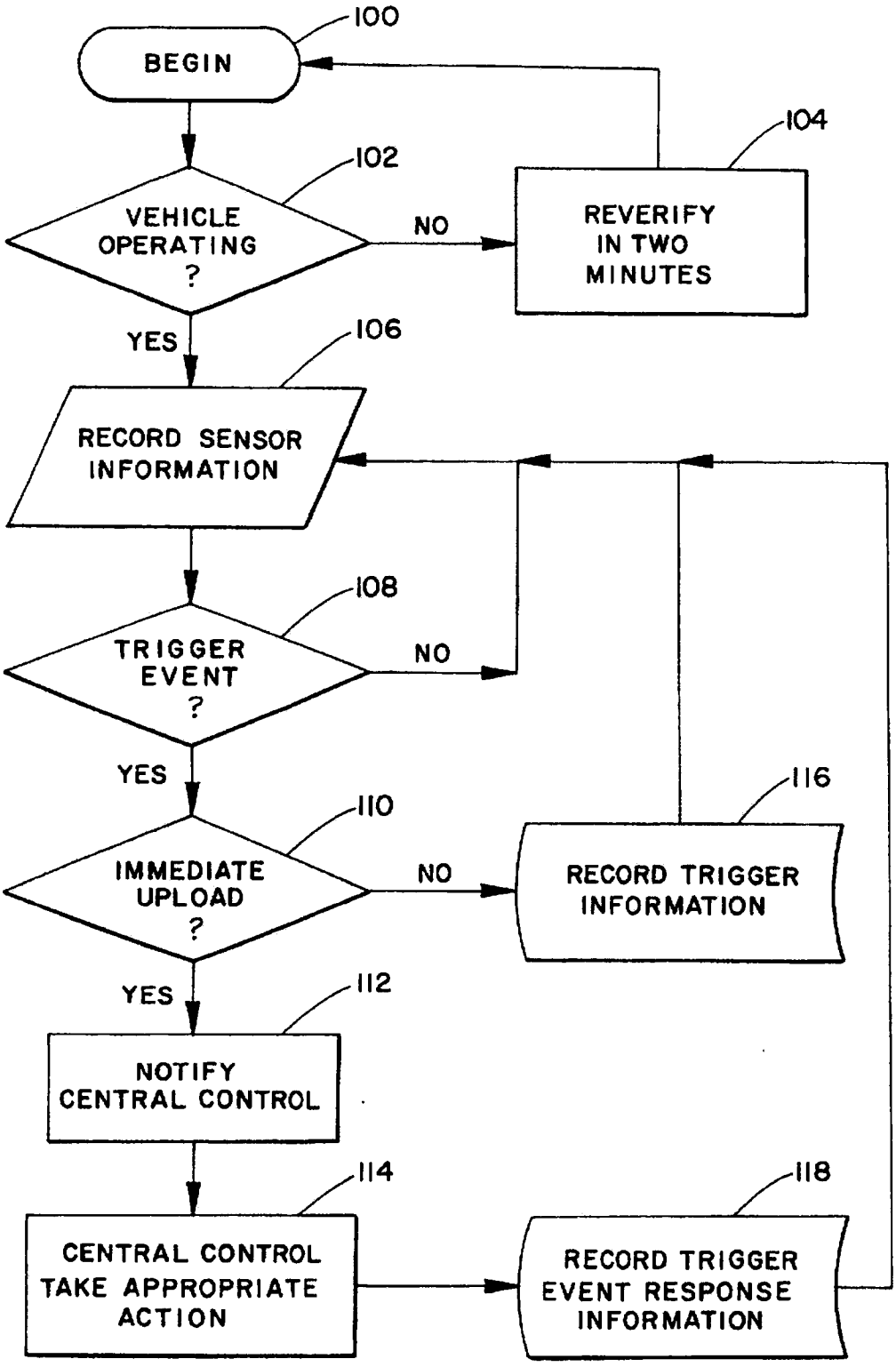
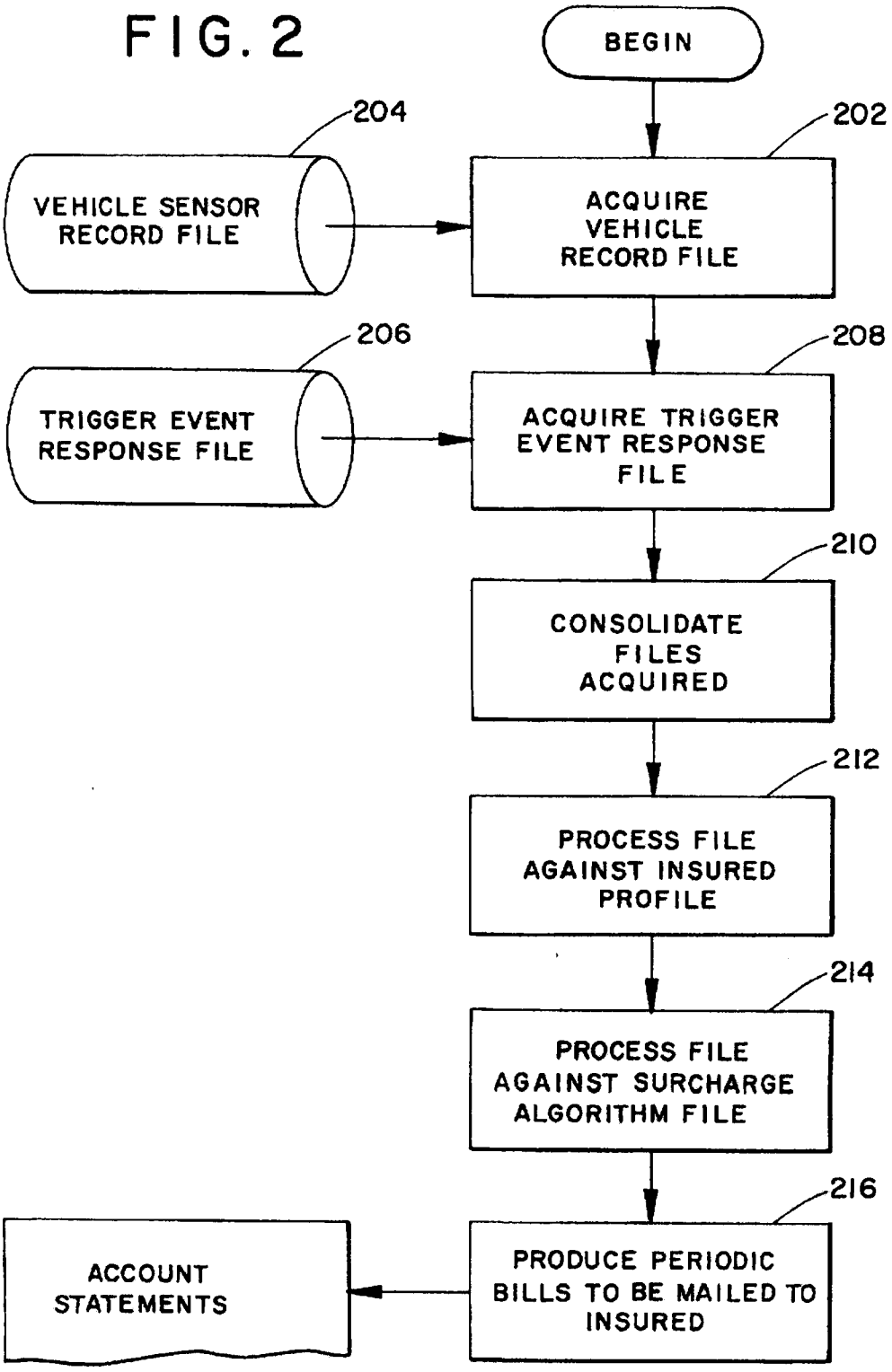

100
BEGIN
102
VEHICLE OPERATING ?
NO
104
REVERIFY IN TWO MINUTES
YES
106
RECORD SENSOR INFORMATION
108
TRIGGER EVENT ?
NO
YES
110
IMMEDIATE UPLOAD ?
NO
116
RECORD TRIGGER INFORMATION
YES
112
NOTIFY CENTRAL CONTROL
114
CENTRAL CONTROL TAKE APPROPRIATE ACTION
118
RECORD TRIGGER EVENT RESPONSE INFORMATION

FIG. 1

FIG. 2


BEGIN
204
202
VEHICLE SENSOR RECORD FILE
ACQUIRE VEHICLE RECORD FILE
206
208
TRIGGER EVENT RESPONSE FILE
ACQUIRE TRIGGER EVENT RESPONSE FILE
210
CONSOLIDATE FILES ACQUIRED
212
PROCESS FILE AGAINST INSURED PROFILE
214
PROCESS FILE AGAINST SURCHARGE ALGORITHM FILE
216
ACCOUNT STATEMENTS
PRODUCE PERIODIC BILLS TO BE MAILED TO INSURED

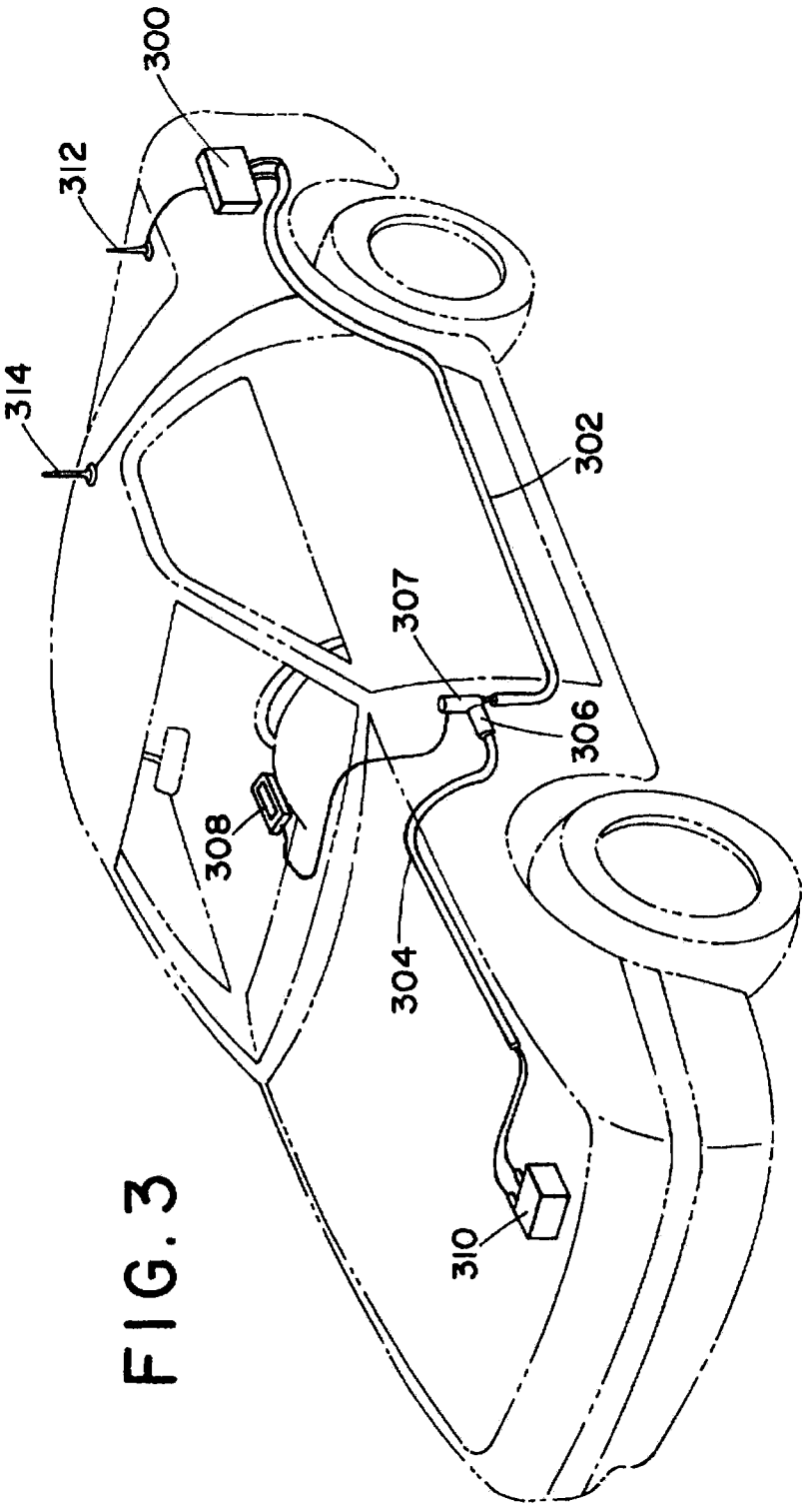


FIG. 3

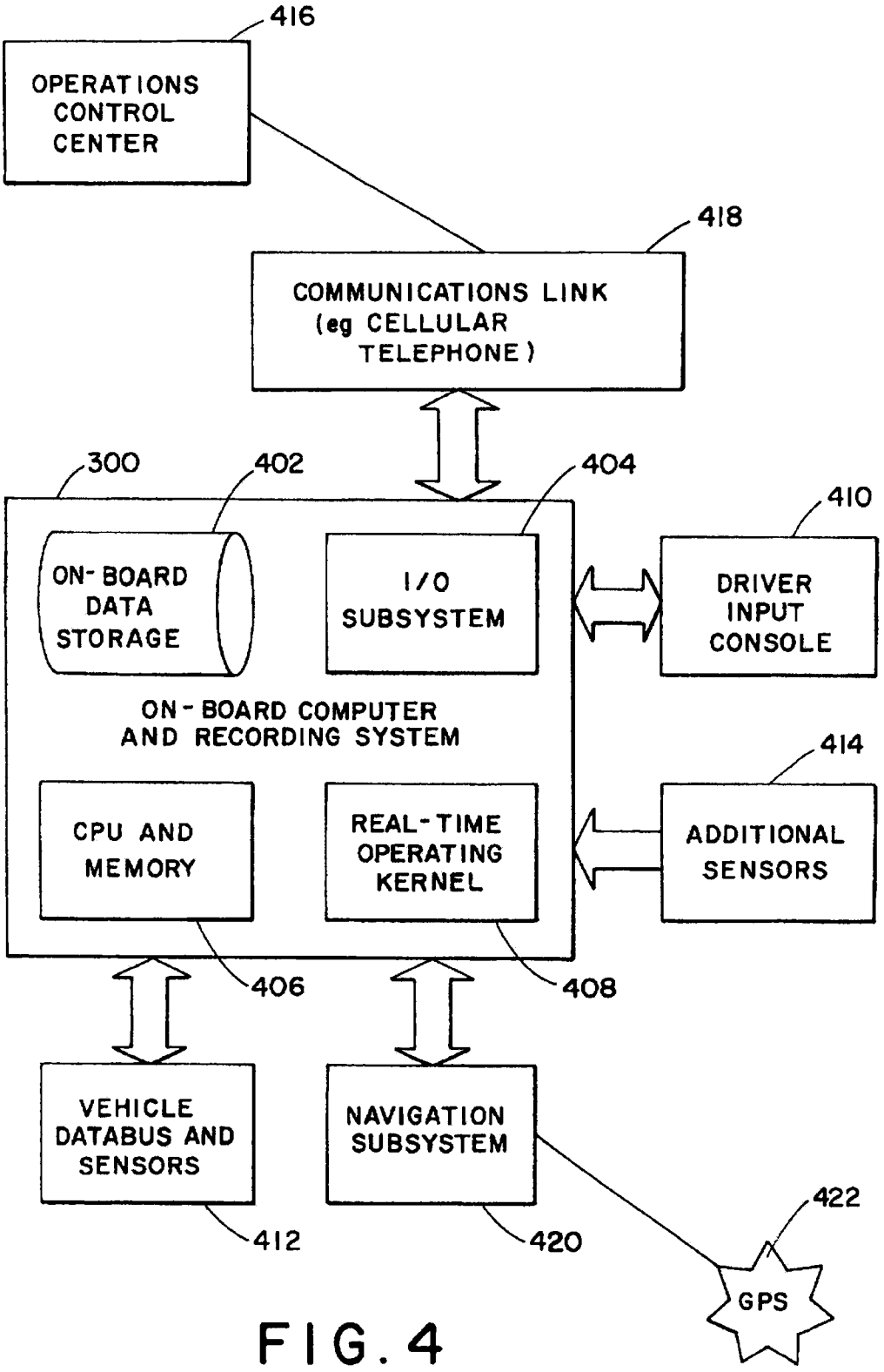
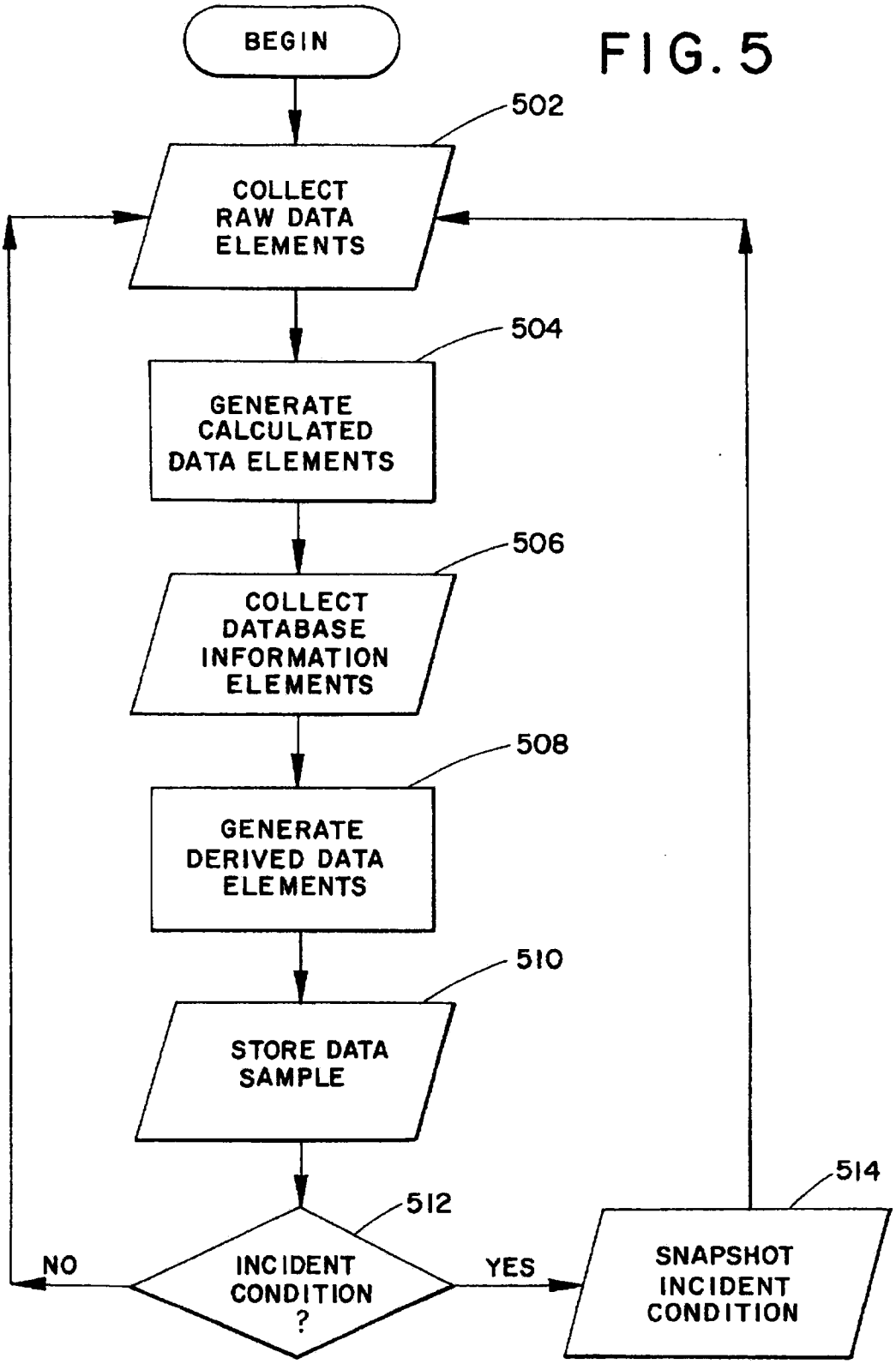

416
OPERATIONS CONTROL CENTER
418
COMMUNICATIONS LINK (eg CELLULAR TELEPHONE)
300
402
404
410
ON-BOARD DATA STORAGE
I/O SUBSYSTEM
DRIVER INPUT CONSOLE
ON-BOARD COMPUTER AND RECORDING SYSTEM
414
CPU AND MEMORY
REAL-TIME OPERATING KERNEL
ADDITIONAL SENSORS
406
408
VEHICLE DATABUS AND SENSORS
NAVIGATION SUBSYSTEM
422
412
420
GPS

FIG. 4

FIG. 5


BEGIN
502
COLLECT RAW DATA ELEMENTS
504
GENERATE CALCULATED DATA ELEMENTS
506
COLLECT DATABASE INFORMATION ELEMENTS
508
GENERATE DERIVED DATA ELEMENTS
510
STORE DATA SAMPLE
512
INCIDENT CONDITION ?
NO
YES
514
SNAPSHOT INCIDENT CONDITION

INFORMATION DATABASE	INTERFACE	SAMPLE RATE
- MAPS - SPEED LIMITS - TRAFFIC SIGNS - HIGHWAY CONDITIONS - (FUTURE TBD)	-COMPUTER STORAGE	- ON DEMAND
VEHICLE SOURCES	**INTERFACE**	**SAMPLE RATE**
- ENGINE DATA - BODY DATA - ELECTRICAL DATA	-SAE J1978 CONNECTOR	- 10-15HZ
OTHER SOURCES	**INTERFACE**	**SAMPLE RATE**
- IVHS DATA - GPS DATA - SECURITY SYSTEM - ADDITIONAL SYSTEM(S)	- VARIOUS I/O PORTS (eg, RS-232/422, ETC.)	- VARIES

FIG. 6

MOTOR VEHICLE INSURANCE PROCESS
VEHICLE DATA ACQUISITION PROCESS FLOW

MOTOR VEHICLE MONITORING SYSTEM FOR DETERMINING A COST OF INSURANCE

BACKGROUND OF THE INVENTION

The present invention relates to data acquisition and processing systems, and particularly to a system for monitoring motor vehicle operational characteristics and driver behavior to obtain increased amounts of data relating to the safety of use for purposes of providing a more accurate determination of a cost of insurance for the vehicle.

Conventional methods for determining costs of motor vehicle insurance involve gathering relevant historical data from a personal interview with the applicant for the insurance and by referencing the applicant's public motor vehicle driving record that is maintained by a governmental agency, such as a Bureau of Motor Vehicles. Such data results in a classification of the applicant to a broad actuarial class for which insurance rates are assigned based upon the empirical experience of the insurer. Many factors are relevant to such classification in a particular actuarial class, such as age, sex, marital status, location of residence and driving record.

The current system of insurance creates groupings of vehicles and drivers (actuarial classes) based on the following types of classifications.

Vehicle:

Age;

manufacturer, model; and

value.

Driver:

Age;

sex;

marital status;

driving record (based on government reports), violations (citations);

at fault accidents; and

place of residence.

Coverage:

Types of losses covered, liability, uninsured motorist, comprehensive, and collision;

liability limits; and

deductibles.

The classifications, such as age, are further broken into actuarial classes, such as 21 to 24, to develop a unique vehicle insurance cost based on the specific combination of actuarial classes for a particular risk. For example, the following information would produce a unique vehicle insurance cost.

Vehicle:	
Age	1993 (three years old)
manufacturer, model	Ford, Explorer XLT
value	$18,000.
Driver:	
Age	38 years old
sex	male
marital status	single
driving record (based on government reports)	
violations	1 point (speeding)
at fault accidents	3 points (one at fault accident)
place of residence	33619 (zip code)
Coverage:	
Types of losses covered	
liability	yes
uninsured motorist	no
comprehensive	yes
collision	yes
liability limits	$100,000./$300,000./$50,000.
deductibles	$500./$500.

A change to any of this information would result in a different premium being charged, if the change resulted in a different actuarial class for that variable. For instance, a change in the drivers'age from 38 to 39 may not result in a different actuarial class, because 38 and 39 year old people may be in the same actuarial class. However, a change in driver age from 38 to 45may result in a different premium because of the change in actuarial class.

Current insurance rating systems also provide discounts and surcharges for some types of use of the vehicle, equipment on the vehicle and type of driver. Common surcharges and discounts include:

Surcharges:

Business use.

Discounts:

Safety equipment on the vehicle
airbags, and
antilock brakes;

theft control devices
passive systems (e.g. "The Club"), and
alarm system; and

driver type
good student, and
safe driver (accident free).

A principal problem with such conventional insurance determination systems is that much of the data gathered from the applicant in the interview is not verifiable, and even existing public records contain only minimal information, much of which has little relevance towards an assessment of the likelihood of a claim subsequently occurring. In other words, current rating systems are primarily based on past realized losses. None of the data obtained through conventional systems necessarily reliably predicts the manner or safety of future operation of the vehicle. Accordingly, the limited amount of accumulated relevant data and its minimal evidential value towards computation of a fair cost of insurance has generated a long-felt need for an improved system for more reliably and accurately accumulating data having a highly relevant evidential value towards predicting the actual manner of a vehicle's future operation.

Many types of vehicle operating data recording systems have heretofore been suggested for purposes of maintaining an accurate record of certain elements of vehicle operation. Some are suggested for identifying the cause for an accident, others are for more accurately assessing the efficiency of operation. Such systems disclose a variety of conventional techniques for recording vehicle operation data elements in a variety of data recording systems. In addition, it has also been suggested to provide a radio communication link for such information via systems such as a cellular telephone to provide immediate communication of certain types of data elements or to allow a more immediate response in cases

such as theft, accident, break-down or emergency. It has even been suggested to detect and record seatbelt usage to assist in determination of the vehicle insurance costs (U.S. Pat. No. 4,667,336).

The various forms and types of vehicle operating data acquisition and recordal systems that have heretofore been suggested and employed have met with varying degrees of success for their express limited purposes. All possess substantial defects such that they have only limited economical and practical value for a system intended to provide an enhanced acquisition, recordal and communication system of data which would be both comprehensive and reliable in predicting an accurate and adequate cost of insurance for the vehicle. Since the type of operating information acquired and recorded in prior art systems was generally never intended to be used for determining the cost of vehicle insurance, the data elements that were monitored and recorded therein were not directly related to predetermined safety standards or the determining of an actuarial class for the vehicle operator. For example, recording data characteristics relevant to the vehicle's operating efficiency may be completely unrelated to the safety of operation of the vehicle. Further, there is the problem of recording and subsequently compiling the relevant data for an accurate determination of an actuarial profile and an appropriate insurance cost therefor.

Current motor vehicle control and operating systems comprise electronic systems readily adaptable for modification to obtain the desired types of information relevant to determination of the cost of insurance. Vehicle tracking systems have been suggested which use communication links with satellite navigation systems for providing information describing a vehicle's location based upon navigation signals. When such positioning information is combined with roadmaps in an expert system, vehicle location is ascertainable. Mere vehicle location, though, will not provide data particularly relevant to safety of operation unless the data is combined with other relevant data in an expert system which is capable of assessing whether the roads being driven are high-risk or low-risk with regard to vehicle safety.

The present invention contemplates a new and improved motor vehicle monitoring, recording and communication system, which primarily overcomes the problem of determining cost of vehicle insurance based upon data which does not take into consideration how a specific vehicle is operated. The subject invention will base insurance charges with regard to current material data representative of actual driving characteristics of the vehicle and driver operation to provide a classification rating of the operator and the vehicle in an actuarial class which has a vastly reduced rating error over conventional insurance cost systems. Additionally, the present invention allows for frequent (monthly) adjustment to the cost of coverage because of the changes in operator behavior and driving patterns. This can result in automobile insurance charges that are readily controllable by individual operators. The system is adaptable to current electronic operating systems, tracking systems and communication systems for the improved extraction of selected insurance related data.

BRIEF SUMMARY OF THE INVENTION

In accordance with the present invention, there is disclosed a method of determining a cost of automobile insurance based upon monitoring, recording and communicating data representative of operator and vehicle driving characteristics, whereby the cost is adjustable by relating the driving characteristics to predetermined safety standards. The method is comprised of steps of monitoring a plurality of raw data elements representative of an operating state of a vehicle or an action of the operator. Selected ones of the plurality of raw data elements are recorded when they are determined to have an identified relationship to the safety standards. The recorded elements are consolidated for processing against an insured profile and for identifying a surcharge or discount to be applied to a base cost of automobile insurance. The total cost of insurance obtained from combining the base cost and surcharges or discounts is produced as a final cost to the operator.

In accordance with another aspect of the present invention, the recording comprises identifying a trigger event associated with the raw data elements which has an identified relationship to the safety standards so that trigger information representative of the event is recorded.

In accordance with a more limited aspect of the present invention, the method comprises a step of immediately communicating to a central control station via an uplink, information representative of the trigger event and recording response information generated by the control station.

In accordance with yet another aspect of the present invention, the method comprises steps of generating calculated data elements and derived data elements from the raw data elements, and accumulating the calculated and derived data elements in a recording device.

The present invention will use information acquired from the vehicle to more accurately assess vehicle usage and thereby derive insurance costs more precisely and fairly. Examples of possible actuarial classes developed from vehicle provided data include:

Driver:

Total driving time in minutes by each driver of the insured vehicle;

number of minutes driving in high/low risk locations (high/low accident areas);

number of minutes of driving at high/low risk times (rush hour or Sunday afternoon);

safe driving behavior,
using seat belts,
use of turn signals,
observance of speed limits, and
observance of traffic control devices;

number of sudden braking situations; and

number of sudden acceleration situations.

Vehicle:

Location vehicle is parked at night (in garage, in driveway, on street);

and

location vehicle is parked at work (high theft locations, etc.).

These new and more precise actuarial classes are considered to be better predictors of loss because they are based on actual use of the vehicle and the behaviors demonstrated by the driver. This will allow the consumers unprecedented control over the ultimate cost of their vehicle insurance.

In accordance with the present invention, additional discounts and surcharges based on data provided by the insured vehicle will be available. Examples of surcharges and discounts based on vehicle provided data include:

Surcharges:

Excessive hard braking situations occurring in high risk locations; and

intermittent use of a safety device, such as seat belts.

Discounts:

Regular selection of low/high risk routes of travel;

regular travel at low/high risk times;

significant changes in driving behavior that results in a lower risk;

vacation discount when the vehicle is not used;

regular use of safety devices; and

unfailing observance of speed limits.

There is some overlap between the use of actuarial classes and discounts and surcharges. Until data has been gathered and analyzed it is not possible to determine which vehicle provided data will be used to determine actuarial classes and which will be used for surcharges or discounts.

One benefit obtained by use of the present invention is a system that will provide precise and timely information about the current operation of an insured motor vehicle that will enable an accurate determination of operating characteristics, including such features as miles driven, time of use and speed of the vehicle. This information can be used to establish actual usage based insurance charges, eliminating rating errors that are prevalent in traditional systems and will result in vehicle insurance charges that can be directly controlled by individual operators.

It is another benefit of the subject invention that conventional motor vehicle electronics are easily supplemented by system components comprising a data recording, a navigation system and a communications device to extract selected insurance relevant data from the motor vehicle.

It is yet another object of the present invention to generate actuarial classes and operator profiles relative thereto based upon actual driving characteristics of the vehicle and driver, as represented by the monitored and recorded data elements for providing a more knowledgeable, enhanced insurance rating precision.

The subject new insurance rating system retrospectively adjusts and prospectively sets premiums based on data derived from motor vehicle operational characteristics and driver behavior through the generation of new actuarial classes determined from such characteristics and behavior, which classes heretofore have been unknown in the insurance industry. The invention comprises an integrated system to extract via multiple sensors, screen, aggregate and apply for insurance rating purposes, data generated by the actual operation of the specific vehicle and the insured user/driver.

Other benefits and advantages of the subject new vehicle insurance cost determination process will become apparent to those skilled in the art upon a reading and understanding of the specification.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention may take physical form in certain parts and steps and arrangements of parts and steps, the preferred embodiments of which will be described in detail in this specification and illustrated in the accompanying drawings which form a part hereof and wherein:

FIG. 1 is a flowchart generally describing a data gathering process from a vehicle;

FIG. 2 is a flowchart detailing the gathering and consolidating of appropriate information for determining a cost of insurance and the resulting insurance billing process;

FIG. 3 is a suggestive perspective drawing of a vehicle including certain data element monitoring, recording and communicating devices;

FIG. 4 is a block diagram of a vehicle on-board computer and recording system implementing the subject invention for selective communication with a central control center and a global positioning navigation system;

FIG. 5 is a flowchart generally illustrating a method for acquiring and recording vehicle insurance related data; and

FIG. 6 a tabular illustration of various sources of insurance-related data, a necessary interface for acquiring the data and an exemplary sample rate therefor.

DETAILED DESCRIPTION OF THE INVENTION

Referring now to the drawings, wherein the showings are for purposes of illustrating the preferred embodiments of the invention only and not for purposes of limiting same, the FIGURES show an apparatus and method for monitoring, recording and communicating insurance related data for determination of an accurate cost of insurance based upon evidence relevant to the actual operation and in particular the relative safety of that operation. Generally, a vehicle user is charged for insurance based upon statistical averages related to the safety of operation based upon the insurer's experience with other users who drive similar vehicles in a similar geographic area. The invention allows for the measure of the actual data while the motor vehicle is being driven. Such data measurement will allow the vehicle user to directly control his/her insurance costs by operating the vehicle in a manner which he/she will know will evidence superior safety of operation and a minimal risk of generation of an insurance claim. Examples of data which can be monitored and recorded include:

1. Actual miles driven;
2. Types of roads driven on (high risk vs. low risk); and,
3. Safe operation of the vehicle by the vehicle user through:
   - A. speeds driven,
   - B. safety equipment used, such as seat belt and turn signals,
   - C. time of day driven (high congestion vs. low congestion),
   - D. rate of acceleration,
   - E. rate of braking,
   - F. observation of traffic signs.

With reference to FIG. 3, an exemplary motor vehicle is shown in which the necessary apparatus for implementing the subject invention is included. An on-board computer **300** monitors and records various sensors and operator actions to acquire the desired data for determining a fair cost of insurance. Although not shown therein, a plurality of operating sensors are associated with the motor vehicle to monitor a wide variety of raw data elements. Such data elements are communicated to the computer through a connections cable which is operatively connected to the vehicle data bus **304** through an SAE-J1978 connector, or OBD-II connector or other vehicle sensors **306**. A driver input device **308** is also operatively connected to the computer **300** through connector **307** and cable **302**. The computer is powered through the car battery **310** or a conventional generator system (not shown). Tracking of the vehicle for location identification can be implemented by the computer **300** through navigation signals obtained from a GPS (global positioning system) antenna or other locating system **312**. The communications link to a central control station is accomplished through the cellular telephone, radio, satellite or other wireless communication system **314**.

FIG. 4 provides the block diagram of the in-vehicle computer system. The computer **300** is comprised of four principal components, an on-board data storage device **402**,

an input/output subsystem **404** for communicating to a variety of external devices, a central processing unit and memory device **406** and a real time operating kernel **408** for controlling the various processing steps of the computer **300**. The computer **300** essentially communicates with three on-board vehicle devices for acquisition of information representative of various actual vehicle operating characteristics. A driver input console **410** allows the driver to input data representative of a need for assistance or for satisfaction of various threshold factors which need to be satisfied before the vehicle can be operated. The physical operation of the vehicle is monitored through various sensors **412** in operative connection with the vehicle data bus, while additional sensors **414** not normally connected to the data bus can be in direct communication with the computer **300** as will hereinafter be more fully explained.

The vehicle is linked to an operation control center **416** by a communications link **418**, preferably comprising a conventional cellular telephone interconnection. A navigation sub-system **420** receives radio navigation signals from a GPS **422**.

The type of elements monitored and recorded by the subject invention comprise raw data elements, calculated data elements and derived data elements. These can be broken down as follows:

Raw Data Elements:

Power train sensors
- RPM,
- transmission setting (Park, Drive, Gear, Neutral),
- throttle position,
- engine coolant temperature,
- intake air temperature,
- barometric pressure;

Electrical sensors
- brake light on,
- turn signal indicator,
- headlamps on,
- hazard lights on,
- back-up lights on,
- parking lights on,
- wipers on,
- doors locked,
- key in ignition,
- key in door lock,
- horn applied;

Body sensors
- airbag deployment,
- ABS application,
- level of fuel in tank,
- brakes applied,
- radio station tuned in,
- seat belt on,
- door open,
- tail gate open,
- odometer reading,
- cruise control engaged,
- anti-theft disable;

Other sensors
- vehicle speed,
- vehicle location,
- date,
- time,
- vehicle direction,
- IVHS data sources.

Calculated Data Elements:
- rapid deceleration;
- rapid acceleration;
- vehicle in skid;
- wheels in spin;
- closing speed on vehicle in front;
- closing speed of vehicle in rear;
- closing speed of vehicle to side (right or left);
- space to side of vehicle occupied;
- space to rear of vehicle occupied;
- space to front of vehicle occupied;
- lateral acceleration;
- sudden rotation of vehicle;
- sudden loss of tire pressure;
- driver identification (through voice recognition or code or fingerprint recognition);
- distance travelled; and
- environmental hazard conditions (e.g. icing, etc.).

Derived Data Elements:
- vehicle speed in excess of speed limit;
- observation of traffic signals and signs;
- road conditions;
- traffic conditions; and
- vehicle position.

This list includes many, but not all, potential data elements.

With particular reference to FIG. **1**, a flowchart generally illustrating the data gathering process of the subject invention is illustrated. Such a process can be implemented with conventional computer programming in the real time operating kernel **408** of the computer **300**. The process is identified with initially a begin step **100** (key in ignition?) and a check of whether the vehicle is operating at step **102**. If the vehicle is not operating a reverification occurs every two (2) minutes as shown at step **104**. It should be noted that the computer is continually powered by at least the vehicle battery **310** (FIG. **3**), but it can be appreciated that during operation the generator (not shown) will supply the energy. If the vehicle is operating, then there is a step of recording sensor information **106**. The recording comprises monitoring a plurality of raw data elements, calculated data elements and derived data elements as identified above. Each of these is representative of an operating state of the vehicle or an action of the operator. Select ones of the plurality of data elements are recorded when the ones are determined to have an identified relationship to the safety standards. For example, vehicle speed in excess of a predetermined speed limit will need to be recorded but speeds below the limit need only be monitored and stored on a periodic basis. The recording may be made in combination with date, time and location. Other examples of data needed to be recorded are excessive rates of acceleration or frequent hard braking.

The recording process would be practically implemented by monitoring and storing the data in a buffer for a selected period of time, e.g., thirty seconds. Periodically, such as every two minutes, the status of all monitored sensors for the data elements is written to a file which is stored in the vehicle data storage **402**. The raw, calculated and derived data elements listed above comprise some of the data elements to be so stored.

Certain of the recorded sensor information may comprise a trigger event of which inquiry is identified at step **108**. "Trigger events" are defined as a combination of sensor data requiring additional action or which may result in a surcharge or discount during the insurance billing process. Certain trigger events may require immediate upload **110** to a central control which will then be required to take appro-

priate action. For example, a trigger event would be rapid deceleration in combination with airbag deployment indicating a collision, in which case the system could notify the central control of the vehicle location. Alternatively, if the operator were to trigger on an emergency light, similarly the system could notify the central control of the vehicle location indicating that an emergency is occurring. The trigger information is recorded, as at step **116**, and whatever response is taken by the central control is also recorded at step **118**. The trigger information recording step **116** and the recording sensor information step **106** may impart recording of information in the on-board data storage device **402** or memory **406**. The event response information recording at step **118** will usually occur in the central control station. Such response information could be the dispatch of an emergency vehicle, or the telephoning of police or an EMS unit.

Trigger events are divided into two groups: those requiring immediate action and those not requiring immediate action, but necessary for proper billing of insurance. Those required for proper billing of insurance will be recorded in the same file with all the other recorded vehicle sensor information. Those trigger events requiring action will be uploaded to a central control center which can take action depending on the trigger event. Some trigger events will require dispatch of emergency services, such as police or EMS, and others will require the dispatch of claims representatives from the insurance company.

The following comprises an exemplary of some, but not all, trigger events:

Need for Assistance:

These events would require immediate notification of the central control center.

1. Accident Occurrence. An accident could be determined through the use of a single sensor, such as the deployment of an airbag. It could also be determined through the combination of sensors, such as a sudden deceleration of the vehicle without the application of the brakes.
2. Roadside assistance needed. This could be through the pressing of a "panic button" in the vehicle or through the reading of a sensor, such as the level of fuel in the tank. Another example would be loss of tire pressure, signifying a flat tire.
3. Lock-out assistance needed. The reading of a combination of sensors would indicate that the doors are locked but the keys are in the ignition and the driver has exited the vehicle.
4. Driving restrictions. The insured can identify circumstances in which he/she wants to be notified of driving within restricted areas, and warned when he/she is entering a dangerous area. This could be applied to youthful drivers where the parent wants to restrict time or place of driving, and have a record thereof.

Unsafe Operation of the Vehicle

These events would be recorded in the in-vehicle recording device for future upload. Constant trigger events would result in notification of the driver of the exceptions.

1. Excessive speed. The reading of the vehicle speed sensors would indicate the vehicle is exceeding the speed limit. Time would also be measured to determine if the behavior is prolonged.
2. Presence of alcohol. Using an air content analyzer or breath analyzer, the level of alcohol and its use by the driver could be determined.
3. Non-use of seatbelt. Percent of sample of this sensor could result in additional discount for high use or surcharge for low or no use.
4. Non-use of turn signals. Low use could result in surcharge.
5. ABS application without an accident. High use could indicate unsafe driving and be subject to a surcharge.

With particular reference to FIG. **2**, a general flowchart describing the steps of the gathering of appropriate information for billing insurance on a periodic basis is illustrated.

At the initiation of the vehicle insurance billing process, the central billing system of the insurer will acquire **202** the vehicle sensor record file from the sensor record file **204** from each vehicle to be billed. This process of data acquisition will involve a periodic uploading of the vehicle file **204**. This file will be uploaded to the central system when the storage device **402** in the vehicle approaches capacity, on command, or when the billing process starts. All the information from the combination of files stored in the vehicle will be used to determine the bill for the insurance on the vehicle for the prior insurance period. Data acquisition is also made from the trigger event response file **206** in the acquisition step **208**. This data is stored in the central control center, and includes information for response activities listed above which require additional billing for services rendered to the insured.

At step **210**, the vehicle sensor record file and the trigger event response file are consolidated. Such files will include all the activity for which the insured is to be billed for the prior period. At step **212**, all the information comprising the insured profile, which is already maintained and stored in other insurance files, is applied to the consolidated activity files for the immediately prior period. This insured profile includes the information about coverages including limits and deductibles, which are necessary for establishing the appropriate cost of insurance for the subject insured. At step **214**, the acquired consolidated file information from step **210** and the overall insured profile acquired at step **212** are combined and processed against a surcharge or discount algorithm file, which include the specific factors for the various usage patterns and trigger events. The surcharges and discounts are continuously adjusted based on the loss results associated with driving behaviors demonstrated. Finally at step **216**, the appropriate billing is produced showing the charges for insurance and other services for the prior period. The billing can be sent electronically or in printed form to the insured for payment.

With particular reference to FIG. **5**, a general diagram of the process for acquiring and recording vehicle insurance related data is illustrated. At step **502**, the raw data elements are collected from the vehicle sensors that provide the raw data elements identified above. Calculated data elements are generated in step **504** and derived data elements are generated at step **508**. As noted, it is necessary to collect certain database information elements at step **506** prior to generating the derived data elements. A sample of all the data elements is stored in the vehicle at step **510**. The sample rate or the recording of the information is controlled based upon the particular insurance billing recording needs predetermined by an algorithm developed by the insurance company. The algorithm will change depending on the particular type of insurance related requirements for the information. At step **512**, if a certain incident, for example collision, occurs then a snapshot is generated of all the relevant data elements at the time of the incident, **514**.

With reference to FIG. **6**, various examples of sources of insurance related data, the interface required to acquire the data and an example of the sample rate are illustrated for a preferred embodiment of the subject invention. Accordingly, it can be seen that for a certain information database

comprised of maps, speed limits, traffic signs, and highway conditions is stored in the data storage device of the computer and can be obtained on demand therefrom. Acquiring data from vehicle sources such as engine data, body data and electrical data is obtained through a conventional SAEJ 1978 connector with an exemplary sample rate of 10–15 Hz. The other sources of relevant data, such as IVHs, GPS, security system or any additional systems are obtained through various I/O ports and the sample rate can be varied in accordance with the desired goals of the insurer.

One of the useful consequences of the subject invention is that other products could be marketed to a particular vehicle operator based on information provided from the subject invention from the operator's motor vehicle. Since the invention includes processes for gathering, extracting and analyzing information provided by the vehicle, a more informed judgment can be made about a determination of when and which products could be marketed to that motor vehicle operator. For example, by knowing that a vehicle operator travels on vacation in that vehicle to a certain resort location may give rise to a marketing of a package of products particular to the type of travel or the location. Another example would relate to the knowledge that the vehicle operator attends particular types of sporting events which may give rise to certain types of products catered to fans of that sporting event.

The invention has been described with reference to preferred embodiments. Obviously, modifications and alterations will occur to others upon a reading and understanding of the specification. It is our intention to include all such modifications and alterations insofar as they come within the scope of the appended claims or the equivalents thereof.

Having thus described our invention, we claim:

1. A method of determining a cost of automobile insurance for a selected period based upon monitoring, recording and communicating data representative of operator and vehicle driving characteristics during said period, whereby the cost is adjustable by relating the driving characteristics to predetermined safety standards, the method comprising:

determining an initial insured profile and a base cost of automobile insurance based on said insured profile;

monitoring a plurality of data elements representative of an operating state of a vehicle or an action of the operator during the selected period;

recording selected ones of the plurality of data elements when said ones are determined to have a preselected relationship to the safety standards;

consolidating said selected ones for identifying a surcharge or discount to be applied to the base cost; and,

producing a final cost of automobile insurance for the selected period from the base cost and the surcharge or discount.

2. The method as described in claim 1 wherein said recording comprises identifying a trigger event associated with a one of the data elements having the preselected relationship and recording both the one data element and trigger information representative of the trigger event.

3. The method as described in claim 1 further including immediately communicating to a central control station via an uplink information representative of a trigger event associated with a one of the data elements.

4. The method as described in claim 3 further including recording trigger event response information generated by said control station.

5. The method as described in claim 1 further including generating derived data elements from said data elements.

6. The method as described in claim 5 wherein said consolidating comprises accumulating said calculated and derived data elements.

7. The method as described in claim 1 wherein said monitoring comprises:

calculating a total driving time of the vehicle and classifying relative portions of the driving time amongst a plurality of rating classifications comprising high, medium, and low risk driving times; and

further identifying geographic locations of driving area and classifying the identified geographic location for area of driving amongst a plurality of classifications comprising high, medium, and low risk driving locations.

8. The method as described in claim 7 wherein said consolidating comprises calculation of a percentage of drive time in the drive time classifications and the drive location classifications.

9. The method as described in claim 1 wherein at least a portion of the data elements are within an awareness and selected control of the operator and therein the method further comprises adjusting by an operator of the operator driving characteristics thereby causing a change in the data elements to obtain the discount in the final cost.

10. The method as described in claim 9 wherein the base cost is for a predetermined period of time and wherein the adjusting by the operator is set to occur at predetermined intervals within the predetermined period.

11. The method as described in claim 10 wherein the predetermined period of time comprises two years and the predetermined intervals comprise monthly intervals.

12. A process for acquiring and recording vehicle insurance related data during a time period via an on-board computer and recording system for adjusting an insurance cost during the time period comprising steps of:

monitoring a plurality of data elements representative of vehicle operating states and driver actions during the time period;

recording selected ones of the data elements in a vehicle record file of an on-board data storage device when said ones are identified as having a relationship material to determination of the insurance cost;

identifying whether said selected ones comprise a trigger event, and if so identified, communicating information representative of the trigger event to a central control station for storage in a trigger event file; and,

consolidating said vehicle record file and said trigger event file in a form for determining a vehicle cost of insurance for the time period.

13. The process as defined in claim 12 further including communicating from the central control station an order for dispatch of an emergency or assist vehicle in response to the identifying of a special trigger event determined to require driver assistance.

14. The process as defined in claim 12 wherein said monitoring comprises;

calculating a total driving time of the vehicle and classifying relative portions of the driving time amongst a plurality of rating classifications comprising high, medium, and low risk driving times; and

further identifying geographic locations of driving area and classifying the identified geographic locations for area of driving amongst a plurality of classifications comprising high, medium, and low risk driving locations.

15. The system as defined in claim 12 wherein said consolidating comprises calculation of a percentage of drive time in the drive time classifications and the drive location classifications.

16. A system of determining a cost of automobile insurance for a selected time period based upon monitoring, recording and communicating data representative of operator and vehicle driving characteristics, whereby the cost is adjustable by relating the driving characteristics to predetermined safety standards, the system comprising:

means for predetermining an insured profile and a base cost of automobile insurance based on said insured profile;

means for monitoring a plurality of data elements representative of an operating state of a vehicle or an action of the operator during the selected time period;

means for recording selected ones of the plurality of data elements when said ones are determined to have a preselected relationship to the safety standards;

means for consolidating said selected ones for identifying a surcharge or discount to be applied to the base cost; and,

means for producing a final cost for the selected time period from the base cost and the surcharge or discount.

17. The system as described in claim 16 further including means for immediately communicating to a central control station via an uplink information representative of a trigger event associated with the data elements whereby a dispatch of an emergency vehicle may be selectively made.

18. The system as described in claim 16 further including means for generating calculated data elements.

19. The system as described in claim 18 further including means for generating derived data elements.

20. The system as defined in claim 16 wherein said means for monitoring comprises:

means for calculating a total driving time of the vehicle and classifying relative portions of the driving time amongst a plurality of rating classifications comprising high, medium, and low risk driving times; and

means for further identifying geographic locations of driving area and classifying the identified geographic locations for area of driving amongst a plurality of classifications comprising high, medium, and low risk driving locations.

21. The system as defined in claim 20 wherein said means for consolidating comprises said means for calculating a percentage of drive time in the drive time classifications and the drive location classifications.

22. A method of generating an actuarial class system for determining vehicle insurance costs for adjusting premiums for an insurance period of time based on data derived from motor vehicle operational characteristics and driver behavior during said insurance period of time, comprising:

monitoring a plurality of data elements representing vehicle operating states and driver actions during said insurance period of time;

recording selected ones of the data elements in a vehicle record file when said ones are identified as having a relationship material to determination of a cost of insurance;

setting a plurality of actuarial classes associated with corresponding degrees of safety of operation of the vehicle; and.

consolidating said vehicle record files with selected actuarial classes for determining a corresponding cost of insurance for the vehicle in correspondence with a one of the actuarial classes for the insurance period of time.

23. The process for determining a cost of insurance as defined in claim 22 wherein said monitoring and recording steps occur continuously and concurrently with actual vehicle operation for acquiring the data elements during actual vehicle use.

24. The process for determining a cost of insurance as defined in claim 23 wherein at least a portion of the plurality of data elements are within an awareness and selective control of a driver, the process further comprising adjusting by the driver of driving behavior to change said portion of data elements for matching said vehicle record with an other one of the actuarial classes.

25. An integrated system for extracting data from multiple sensors, and screening, aggregating and applying the data for insurance rating purposes, the data being generated by an actual operation of a specific motor vehicle during a selected data collection period comprising:

means for extracting a plurality of data elements from the multiple sensors wherein the elements are representative of vehicle operating states and driver actions during the selected data collection period;

means for screening the data elements and aggregating selected ones of the data elements in a vehicle record file of an on-board storage device when said selected ones are identified as having a relationship material to determination of a cost of insurance for the vehicle;

means for associating the aggregated selected data elements with predetermined actuarial classes indicative of a degree of safety of operation of the vehicle; and

means for producing a cost of insurance for the selected data collection period.

26. The system as described in claim 25 further including means for generating calculated data elements and derived data elements, said calculated and derived data elements being further aggregated for association with the actuarial classes.

* * * * *

Exhibit 5

SYSTEM OF CHARGING FOR AUTOMOBILE INSURANCE

FIELD OF THE INVENTION

[0001] The present invention relates to a method of charging for vehicle insurance, and more particularly to a method of using location information to charge for vehicle insurance but restricting access to the location information to add to the privacy of the vehicle owner.

BACKGROUND OF THE INVENTION

[0002] Most drivers, if not all, have insurance for their motor vehicle(s) (i.e., cars, trucks, motorcycles, etc.). Many states now mandate that vehicle insurance be purchased and maintained by the vehicle owner. Leasing companies also often require that insurance be maintained on a leased vehicle.

[0003] Insurance companies traditionally obtain background information from the driver and about the driver's vehicle through interviews and applications. The background information is compared to information databases that may include actuarial statistics. From the comparison, a total cost is determined and the driver is charged for the vehicle insurance accordingly. It should be appreciated that unless additional information is reported to the insurance company, for example, accidents or other driver information, no further data may be used to revise the cost of the automobile insurance. Because the insurance company uses little to no new data, for revising the cost of a driver's insurance policy, the cost of the policy may

become incommensurate with the actual risk presented by a given driver/vehicle combination, and the cost to underwrite that risk.

[0004] The conventional way of charging for vehicle insurance, as noted above, presents very little opportunity for the driver to change his or her driving habits to otherwise affect the cost of the vehicle insurance. While avoiding accidents remains a traditional way to keep the cost of insurance low, accidents are only one input in determining the cost of the vehicle insurance. Notwithstanding, some drivers' activity or lack thereof may not be adequately accounted for when establishing the cost for the vehicle insurance policy. Some aforementioned driver activity may include taking advantage of city mass transportation systems, and otherwise leaving the vehicle parked or garaged for the majority of the day. Other activity may include driving through high risk areas where accidents are more likely to occur in given intersections or where theft may be more prevalent. As a consequence, one driver may be undercharged while another driver may be overcharged for the risk experienced by the driver/vehicle and the cost to underwrite that risk. It is desirable to provide a method of charging for automobile insurance that is more accurate and more efficient than the conventional methods. It is additionally desirable to provide a method for charging for vehicle insurance that takes into account how, when, and where the vehicle is driven to better gauge the actual risk presented to a driver/vehicle and the cost to underwrite that risk.

[0005] Knowledge of the exact whereabouts of the vehicle at a given time allows the insurance company to derive more accurately the costs based on that location information. Consumers, however, are wary of

transmitting the exact location of their vehicle on a real-time basis to, among other things, an insurance company. It is desirable to obtain location information to better determine the cost of the vehicle insurance, but otherwise restrict access to the location information and add to the privacy of the operator of the vehicle.

SUMMARY OF THE INVENTION

[0006] The present invention is directed to a system and method for providing real time information concerning various factors on the operation and/or location of a motor vehicle, and using the information to determine an incremental vehicle insurance cost. The incremental vehicle insurance cost represents that cost for vehicle insurance for a given time increment, for example, a single day. This information is transmitted by the system to a remotely located contracting company involved with providing insurance to the vehicle operator.

[0007] In one preferred form, the system includes a computation device that is located on the operator's vehicle. The computation device may monitor one or more factors relating to the operation of the vehicle, such as the vehicle's real time geographic location, its speed, acceleration, deceleration, length of time within certain predefined geographic areas, etc. This information is used along with a suitable cost database and a cost calculation system to generate incremental vehicle insurance cost information that is transmitted to the remote contracting company. In another preferred form, only the vehicle operational information is transmitted to the remotely

located contracting company and the incremental vehicle insurance cost information is determined by the contracting company or a different entity.

[0008] In a preferred implementation the vehicle's operational information is encrypted and stored in a suitable database. In yet another implementation the encrypted information is only available to the vehicle operation and/or the contracting company if a plurality of passwords are employed, one being known only to the vehicle operator and one being known only to the contracting company. This facilitates access to the encrypted information only when both the operator and the contracting company agree that review of such information is needed, such as in the event of a billing dispute.

[0009] The present invention makes it possible to provide an operator of a motor vehicle with near real time incremental insurance cost information which can help assist the operator in modifying driving habits, if needed, to potentially reduce the overall insurance cost associated with operating the vehicle. The invention also enables insurance companies to even more accurately gauge the risk associated with the operation of vehicles that they are insuring so that insurance premiums assessed to operators of motor vehicles can even more accurately reflect the level of risk associated with the operation of each vehicle.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The present invention will become more fully understood from the detailed description, the appended claims, and the accompanying drawings, wherein:

[0011] Figure 1 is a simplified block diagram representing the components of the insurance cost computation system constructed in accordance with the principles of the present invention; and

[0012] Figure 2 is a block diagram representing the components of the computation device of Figure 1 showing inputs and outputs of the computation device.

DETAILED DESCRIPTION OF THE PRESENT INVENTION

[0013] The following description of the present invention is merely exemplary in nature and is in no way intended to limit the invention, its application, or uses.

[0014] With reference to Figure 1, an insurance cost computation system is generally indicated by reference numeral 10. A user 12 operates a vehicle 14 that is either required to be covered by insurance, or for which the user has chosen to purchase insurance coverage. The user 12 contacts a contracting company 16 for example, an automobile insurance company, and elects a pay as you go insurance plan. It should be appreciated that there are many ways to implement the pay as you go insurance plan; however, the present invention, in one preferred form, involves installation of a computation device 18 in the vehicle 14. The computation device 18 may establish a communication link with the contracting company 16, and with an external location identification system 20. The computation device 18 monitors the real time location of the vehicle 14 and determines a cost for the vehicle insurance. This cost is transmitted to the contracting company 16 for later billing to the user 12.

[0015] The computation device 18 may transmit cost information to the contracting company 16 for later billing to the user 12 at various time increments. In one preferred implementation, the computation device 18 contacts the contracting company 16 on a daily basis to transmit cost information. A user interface 22 is available for the user 12 to contact the contracting company 16 and monitor the cost of the vehicle insurance whenever needed. The computation device 18 only transmits the cost information to the contracting company 16; as such, the user interface 22 will only display the cost of the automobile insurance for the given time increment. As noted earlier, if the given time increment is one day, the user 12 may retrieve from the user interface 22 the daily cost of the automobile insurance.

[0016] The computation device 18 may also establish communication with the external location identification system 20. The external location identification system 20 transmits information to the computation device 18 from which the computation device 18 may determine the location of the vehicle 14. The location of the vehicle 14, among other factors, is used to compute the cost of the automobile insurance for the given time increment.

[0017] With reference to Figure 2, a more detailed view of the computation device 18 is shown along with the various systems that may communicate with the computation device 18. The computation device 18 includes an internal location identification system 24 that receives information from the external location identification system 20 via electromagnetic wave signals. In one preferred implementation, the external location identification system 20 comprises a plurality of global positioning system satellites. The

internal location identification system 24 may also comprise a modified global positioning system receiver. The internal location identification system 24 determines the geographical location of the car and correlates that information with a cost lookup database 26. The location information is then encrypted and stored in an encrypted location data system 32. Cost information is tallied by a cost calculation system 28, and then sent to a billing transmission system 30 for eventual transmission of the cost information or a cost increment to the contracting company 16.

[0018] The internal location identification system 24 may provide many features to the computation device 18. For example, the internal location identification system 24 may provide location information and vehicle information. The location information preferably includes one or more pieces of information including a geographical location of the vehicle, a duration of time the vehicle is located within a given geographical location, a vehicle speed, an applicable speed limit, or combinations and derivations thereof. The vehicle information may also include a vehicle acceleration rate, a vehicle deceleration rate, a vehicle maintenance status, an engine speed, a brake force, a vehicle payload, or combinations and derivations thereof.

[0019] The location information and the vehicle information are then evaluated relative to the cost lookup database 26. The cost lookup database 26 may include actuarial statistics and may also include additional information to make the determination of risk for the contracting company 16 more accurate. The additional information in the cost lookup database 26 may include crime statistics, accident statistics, traffic congestion information, weather information, or combinations and derivations thereof. In one

preferred form, the information contained within the cost lookup database 26 is resident within the computation device 18. Additionally, the information contained within the cost lookup database 26 may be updated by the contracting company 16.

[0020] The cost increment is determined by evaluating the location information and the vehicle information along with the cost lookup database 26. The location information and the vehicle information may take the form of a single variable or a plurality of variables with certain values determined by the vehicle and where the vehicle travels. The plurality of variables are ultimately correlated with the cost lookup database 26. In addition, the plurality of variables may comprise absolute mileage, hours driven, multipliers associated with geographic indicators, vehicle indicators, or combinations and derivations thereof.

[0021] The plurality of variables are then associated with the cost lookup database 26, which may comprise multipliers based on mileage or duration, fixed costs associated with the plurality of variables, or combinations or derivations thereof. After the plurality of variables from the location information and the vehicle information are correlated with the cost lookup database 26, a cost increment is produced.

[0022] The cost increment is sent to the cost calculation system 28. The cost increment, therefore, is defined as an amount of money or, put another way, contains only monetary information. More notably, the cost increment excludes any of the location information or the vehicle information. It should be appreciated that the cost increment need only be derived from location information or vehicle information. As such, the computation device

18 can accommodate one or more inputs into the determination of the cost increment.

[0023] The location information and the vehicle information, which are used to derive the cost increment, are saved in the encrypted location data system 32. The cost increment, being only a dollar amount, is passed to the billing transmission system 30, which sends the cost increment to the contracting company 16. The billing transmission system 30 may be configured in many different ways to transmit the cost increment to the contracting company 16. One such configuration is a cellular transmission system using cell phone service. Other exemplary configurations include contacting the contracting company 16 using various forms of electro-magnetic wave communication, a phone connection, an internet connection, and combinations thereof.

[0024] It will be appreciated that the billing transmission system 30 may contact the contracting company at various times. In one preferred form the billing transmission system 30 contacts the contracting company 16 to transmit the cost increment on a daily basis. The billing transmission system 30, however, may contact the contracting company 16 at any time or simply store the billing information until contact is possible.

[0025] As noted earlier, no location information is transmitted to the contracting company 16 on a regular basis. Situations may arise, however, where review of the location information is necessary, such as for billing disputes. Access to the encrypted location data system 32 and subsequent decryption is possible through a dispute access system 36. It should be appreciated that the dispute access system 36 may be configured in many

different ways. Preferably, however, access to the dispute access system 36 only provides access to unencrypted location information when a user password 38 from the user 12 is combined with a contracting company password 34 from the contracting company 16. As such, the only way to decrypt or gain access to the stored location information in the encrypted location data system 32 is with access by a passkey containing at least both passwords 38 and 34. It will be appreciated that both passwords 38 and 34 must be used to access the dispute access system 36.

[0026] It will be appreciated that access to the dispute access system 36 is not unlike conventional safe deposit boxes found at banking institutions. Traditional safe deposit boxes require key access with two keys simultaneously. The first key is held by the safety deposit box holder usually a customer of the bank. The second key is held by the bank. Only when the bank confirms the identity of the customer are both keys used simultaneously to open the safety deposit box. It will be appreciated that the dispute access system 36 may be configured in many different ways, but it is envisioned that the dual password system or dual passkey system may have similarities to systems of accessing a conventional safety deposit vault.

[0027] The dispute access system 36 may be further configured to allow the user 12 to access encrypted location information from the encrypted location data system 32. The user interface 22 may be configured to permit the user 12 to access location information to monitor use and cost associated with driving the vehicle 14. The dispute access system 36 may also be configured to allow access only to unencrypted location information and only in the event of a dispute where access is obtained by the user 12 and the

contracting company 16 simultaneously to reveal the unencrypted location information. The dispute access system 36 may be additionally configured to erase the location information every two months or at any suitable, periodic time increment unless established otherwise, such as in the event of a billing dispute. It should be appreciated that only the user 12 has access to the unencrypted location information. The user 12 may also grant access to the contracting company 16 by combining the user password 38 with the contracting company password 34, thus utilizing the two password or passkey system.

[0028] Because the user 12 is able to access the cost increment or cost information through the user interface 22, the user is able to alter use and activity of the vehicle 14 to possibly reduce the cost of the vehicle insurance. The ability to access the cost of the vehicle insurance on a daily basis empowers the vehicle owner to alter driving habits accordingly, which may result in a savings due to changes in vehicle insurance cost. Furthermore, the contracting company 16 receives much more data about vehicle use over time. The additional data received from the insurance cost computation system 10 may be used to streamline and improve the efficiency of the automobile insurance business to the betterment of the automobile insurance customers as well as to stockholders of insurance companies.

[0029] It will be appreciated that the computation device 18 has a single input which may take the form of information from the external location identification system 20, and a single output which is cost information transmitted from the billing transmission system 30 to the contracting company 16. Only when the user 12 and the contracting company 16 utilize

the dispute access system 36 with both passwords 38 and 34 is additional communication with the computation device 18 realized.

[0030] As noted above, access to the computation device through the dispute access system 36 is the only way to obtain unencrypted location information from the computation device 18. Because only cost information is transmitted from computation device 18, privacy concerns surrounding real time location of the vehicle are accommodated as the computation device 18 only transmits a dollar amount.

[0031] In an alternative implementation, the insurance cost computation system 10 may broadcast raw location information and vehicle information to the contracting company 16, for subsequent cost calculation at the contracting company 16. Further, the plurality of variables derived from the location information and the vehicle information may be transmitted to the contracting company 16. The cost increment could then be determined at the contracting company 16. Notwithstanding the various alternative implementations of the present invention, the preferred implementation only transmits a cost increment to the contracting company 16 and retains and encrypts privacy sensitive information.

[0032] Also, while the computation device 18 is depicted in Figure 2 as a single unit that can be installed, replaced, or swapped accordingly, it will be appreciated that the computation device 18 may be what is conventionally known as a line replaceable unit (LRU). Configuration as an LRU enables the computation device to be quickly and easily removed from a vehicle should the need arise.

[0033] While various embodiments of the present invention have been described, those skilled in the art will recognize modifications or variations which might be made without departing from the inventive concept. The examples illustrate the invention and are not intended to limit it. Therefore, the description and claims should be interpreted liberally with only such limitation as is necessary in view of the pertinent prior art.

CLAIMS

What is claimed is:

1. A method of calculating automobile insurance including a device to monitor a vehicle and communicate with a contracting company comprising:

acquiring location information of the vehicle with a location system;

deriving a cost increment by evaluating at least said location information and a pricing database; and

transmitting said cost increment to the contracting company, wherein said cost increment essentially consists of monetary information.

2. The method of calculating automobile insurance of Claim 1, further comprising acquiring vehicle information.

3. The method of calculating automobile insurance of Claim 2 wherein said cost increment is devoid of at least one of said location information and said vehicle information.

4. The method of calculating automobile insurance of Claim 2, wherein said location information includes at least one of a geographical location of the vehicle, a duration of time the vehicle is located at said geographical location, a vehicle speed, an applicable speed limit, and combinations thereof.

5. The method of calculating automobile insurance of Claim 2, wherein said vehicle information includes at least one of a vehicle speed, a vehicle acceleration rate, a vehicle deceleration rate, a vehicle maintenance status, an engine speed, a brake force, a vehicle payload, and combination thereof.

6. The method of calculating automobile insurance of Claim 2, further comprising restricting access to at least one of said location information and said vehicle information.

7. The method of calculating automobile insurance of Claim 2, further comprising accessing at least one of said location information and said vehicle information with an access key, wherein said access key consists of at least two passkeys.

8. The method of calculating automobile insurance of Claim 7, wherein a first passkey is retained by a customer and a second passkey is retained by the contracting company.

9. The method of calculating automobile insurance of Claim 1, wherein said location system includes at least one of a global positioning satellite receiver to determine location and a geographical database configured to be resident on the device.

10. The method of calculating automobile insurance of Claim 1, wherein said pricing database at least includes actuarial statistics.

11. The method of calculating automobile insurance of Claim 2, further comprising encrypting at least one of said location information and said vehicle information.

12. The method of calculating automobile insurance of Claim 2, further comprising decrypting at least one of said location information and said vehicle information with an access key, wherein said access key consists of at least two passkeys.

13. The method of calculating automobile insurance of Claim 1, further comprising providing user access to said cost increment.

14. The method of calculating automobile insurance of Claim 13, wherein said user access includes at least one of internet web site interface, a phone interface, a customer service interface, and combinations thereof.

15. The method of calculating automobile insurance of Claim 1, wherein transmitting said cost increment includes at least one of establishing a cellular phone connection, establishing a radio connection, establishing microwave communication, establishing a phone connection, establishing an internet connection, and combinations thereof.

16. A vehicle insurance computation device that is installed in a vehicle and communicates with a contracting company comprising:

a computation device configured to acquire location information of the vehicle and derive a cost increment by evaluating at least said location information and a pricing database; and

a transmitting device to send said cost increment to the contracting company, wherein said cost increment essentially consists of monetary information.

17. The vehicle insurance computation device of Claim 16 wherein said computation device is further configured to acquire vehicle information.

18. The vehicle insurance computation device of Claim 17 wherein said cost increment is devoid of at least one of said location information and said vehicle information.

19. The vehicle insurance computation device of Claim 17, wherein said location information includes at least one of a geographical location of the vehicle, a duration of time the vehicle is located at said geographical location, a vehicle speed, an applicable speed limit, and combinations thereof.

20. The vehicle insurance computation device of Claim 17, wherein said vehicle information includes at least one of a vehicle speed, a vehicle acceleration rate, a vehicle deceleration rate, a vehicle maintenance status, an engine speed, a brake force, a vehicle payload, and combinations thereof.

21. The vehicle insurance computation device of Claim 17, further comprising an access device that is configured to provide access to said at least one of said location information and said vehicle information with an access key, wherein said access key consists of at least two passkeys.

22. The vehicle insurance computation device of Claim 21, wherein a first passkey is retained by a customer and a second passkey is retained by the contracting company.

23. The vehicle insurance computation device of Claim 16, wherein said computation device includes at least one of a global positioning satellite receiver to determine location and a geographical database configured to be resident on the device.

24. The vehicle insurance computation device of Claim 23, wherein said pricing database at least includes actuarial statistics.

25. The method of calculating automobile insurance of Claim 17, wherein at least one of said location information and said vehicle information are encrypted.

26. The vehicle insurance computation device of Claim 21 wherein said access device is configured to decrypt at least one of said location information and said vehicle information with said access key.

27. The vehicle insurance computation device of Claim 16, further comprising a user access system configured to provide user access to said cost increment.

28. The vehicle insurance computation device of Claim 27, wherein said user access system includes at least one of internet web site interface, a phone interface, a customer service interface, and combinations thereof.

29. The vehicle insurance computation device of Claim 16, wherein said transmitting device includes at least one of a cellular phone connection, a radio connection, microwave communication, a phone connection, an internet connection, and combinations thereof.

30. A method of determining a cost of insuring a motor vehicle, comprising:

using a monitoring apparatus located on-board the motor vehicle to at least assist in monitoring an operational factor associated with the vehicle in real time;

recording information relating to said operational factor; and

using said recorded information to determine an incremental insurance cost for said motor vehicle related to a given incremental time period.

31. The method of claim 30, further comprising having an underwriting entity provide the operator with a charge for an insuring said vehicle, based on said incremental insurance cost, for said given incremental time period.

32. The method of claim 30, wherein determining an incremental insurance cost comprises using a cost calculation system and a cost lookup database having actuarial information, in addition to said recorded information.

33. The method of claim 30, wherein monitoring an operational factor of said vehicle comprises monitoring at least one of the group of variable comprising:

a speed of said vehicle;

a geographic location of said vehicle;

an acceleration of said vehicle; and

a deceleration of said vehicle.

34. The method of claim 33, further comprising using an external location identification system for assisting in determining a geographic location of said vehicle.

ABSTRACT OF THE DISCLOSURE

A method and apparatus for determining an incremental cost of insurance for the operation of a motor vehicle and billing the same to an operator of the vehicle. The system uses an internal system for determining one or more operational factors associated with the vehicle, such as its geographic location, speed, acceleration, etc, in at least near real time, and recording the information in a database. From this information incremental insurance cost information is determined relating to the cost of insuring the vehicle for a predetermined time during, for example one day. The insurance cost information is transmitted to a contracting company, which may comprise an underwriting company responsible for providing the insurance coverage for the vehicle. The invention makes it possible for an operator to better gauge how driving habits and/or usage of the vehicle affect the cost of the insurance, as well as providing insurance companies with near real time information from which even more accurate determinations of risk can be made, and insurance costs to the operator adjusted accordingly.

Exhibit 6

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	10/674,929
Filing Date:	September 30, 2003
Applicant:	Rodney B. Kendrick
Group Art Unit:	3626
Examiner:	Sheetal R. Rangrej
Title:	SYSTEM OF CHARGING FOR AUTOMOBILE INSURANCE
Attorney Docket:	7784-000652

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

AMENDMENT

Madam:

In response to the Office Action mailed July 25, 2007, please amend the application as follows and consider the remarks set forth below.

Amendments to the Claims begin on page 2 of this paper.

Amendments to the Drawings begin on page 13 of this paper.

Remarks begin on page 14 of this paper.

AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions and listings of claims in the application.

LISTING OF CLAIMS

1. A method of calculating automobile insurance for a vehicle of a customer of ~~including a device to monitor a vehicle and communicate with~~ a contracting company, the method comprising:

acquiring location information of the vehicle with a location system on the vehicle;

acquiring vehicle performance information from the vehicle;

deriving a first cost increment by evaluating at least said location information, said vehicle performance information and a pricing database, wherein said deriving of said first cost increment is performed on the vehicle; ~~and~~

connecting a billing transmission system on the vehicle with the contracting company;

transmitting said first cost increment from the billing transmission system to the contracting company, wherein said first cost increment ~~essentially consists of monetary information~~ is devoid of said location information and said vehicle performance information;

restricting access to by at least encrypting said location information and said vehicle performance information;

accessing by at least decrypting said location information and said vehicle performance information with an access key, wherein said access key consists of

a first passkey retained by the customer and a second passkey retained by the contracting company;

providing access for the customer outside of the vehicle to said first cost increment prior to the contracting company billing the customer, wherein said providing access to said first cost increment is adapted to permit the customer to alter driving habits to adjust a second cost increment;

transmitting said second cost increment from the billing transmission system to the contracting company, wherein said second cost increment is devoid of said location information and said vehicle performance information; and

preparing billing for the customer from the contracting company based on at least said first and said second cost increments.

2. (CANCELED)

3. (CANCELED)

4. (Currently Amended) The method of calculating automobile insurance of Claim 1 [[2]], wherein said location information includes at least one of a geographical location of the vehicle, a duration of time the vehicle is located at said geographical location, a vehicle speed, an applicable speed limit, and combinations thereof.

5. (Currently Amended) The method of calculating automobile insurance of Claim 1 [[2]], wherein said vehicle performance information includes at least one of a vehicle speed, a vehicle acceleration rate, a vehicle deceleration rate, a vehicle maintenance status, an engine speed, a brake force, a vehicle payload, and combination thereof.

6. – 8. (CANCELED)

9. (Original) The method of calculating automobile insurance of Claim 1, wherein said location system includes at least one of a global positioning satellite receiver to determine location and a geographical database configured to be resident on the device.

10. (Original) The method of calculating automobile insurance of Claim 1, wherein said pricing database at least includes actuarial statistics.

11 – 13. (CANCELED)

14. (Currently Amended) The method of calculating automobile insurance of Claim 1 [[13]], wherein said providing ~~user~~ access for the customer to said first cost increment includes at least one of internet web site interface, a phone interface, a customer service interface, and combinations thereof.

15. (Currently Amended) The method of calculating automobile insurance of Claim 1, wherein transmitting said first cost increment includes at least one of establishing a cellular phone connection, establishing a radio connection, establishing microwave communication, establishing a phone connection, establishing an internet connection, and combinations thereof.

16. (Currently Amended) A vehicle insurance computation apparatus ~~device~~ that is installed in a vehicle and communicates with a contracting company that is remote to the vehicle and provides billing to a customer, the vehicle insurance computation apparatus comprising:

a computation device ~~configured to acquire~~ that acquires location information of the vehicle, acquires vehicle performance information from the vehicle and ~~derive~~ derives a first cost increment by evaluating at least said location information, said performance information and a pricing database; and

a transmitting device ~~to send~~ that sends said first cost increment to the contracting company, wherein said first cost increment ~~essentially consists of monetary information~~ is devoid of said location information and said vehicle performance information,

wherein access to said performance information and said location information of the vehicle is restricted by at least encrypting said location information and said vehicle performance information,

wherein access is granted by at least decrypting said location information and said vehicle performance information with an access key,

wherein said access key consists of a first passkey retained by the customer and a second passkey retained by the contracting company,

wherein said computation device is configured to provide access for the customer outside of the vehicle to said first cost increment prior to the billing of the customer by contracting company,

wherein said access for the customer outside of the vehicle to said first cost increment is adapted to permit the customer to alter driving habits to adjust a second cost increment;

wherein said transmitting device sends said second cost increment to the contracting company,

wherein said second cost increment is devoid of said location information and said vehicle performance information, and

wherein said sending of said second cost increment to the contracting company permits the contracting company to prepare the billing for the customer based on at least said first and said second cost increments.

17. (CANCELED)

18. (CANCELED)

19. (Currently Amended) The apparatus ~~vehicle insurance computation device~~ of Claim 16 [[17]], wherein said location information of the vehicle includes at least one of a geographical location of the vehicle, a duration of time the vehicle is located at said geographical location, a vehicle speed, an applicable speed limit, and combinations thereof.

20. (Currently Amended) The apparatus ~~vehicle insurance computation device~~ of Claim 16 [[17]], wherein said ~~vehicle~~ performance information of the vehicle includes at least one of a vehicle speed, a vehicle acceleration rate, a vehicle deceleration rate, a vehicle maintenance status, an engine speed, a brake force, a vehicle payload, and combinations thereof.

21. (CANCELED)

22. (CANCELED)

23. (Currently Amended) The apparatus ~~vehicle insurance computation device~~ of Claim 16, wherein said computation device includes at least one of a global positioning satellite receiver to determine location and a geographical database configured to be resident on the device.

24. (Currently Amended) The apparatus ~~vehicle insurance computation device~~ of Claim 23, wherein said pricing database at least includes actuarial statistics.

25. (CANCELED)

26. (CANCELED)

27. (CANCELED)

28. (Currently Amended) The apparatus ~~vehicle insurance computation device~~ of Claim 16 [[27]], wherein said computation device is configured to provide access for the customer outside of the vehicle through ~~user access system includes~~ at least one of an internet web site interface, a phone interface, a customer service interface, and combinations thereof.

29. (Currently Amended) The apparatus ~~vehicle insurance computation device~~ of Claim 16, wherein said transmitting device includes at least one of a cellular phone connection, a radio connection, microwave communication, a phone connection, an internet connection, and combinations thereof.

30. (Currently Amended) A method of determining a cost of insuring a motor vehicle, comprising:

using a monitoring apparatus located on-board the motor vehicle to at least assist in monitoring an operational factor associated with the motor vehicle in real time;

recording information relating to said operational factor; ~~and~~

~~using said recorded information to determine an~~ determining a first incremental insurance cost with said recorded information for the motor vehicle related to a given incremental time period;

transmitting said first incremental insurance cost to the contracting company, wherein said first incremental insurance cost is devoid of said operational factor;

restricting access to by at least encrypting said operational factor;

accessing by at least decrypting said operational factor with an access key, wherein said access key consists of a first passkey retained by the customer and a second passkey retained by the contracting company;

providing access for the customer outside of the motor vehicle to said first incremental insurance cost prior to the contracting company billing the customer, wherein said providing access to said first incremental insurance cost is adapted to permit the customer to alter driving habits to adjust a second incremental insurance cost;

transmitting said second incremental insurance cost to the contracting company, wherein said second incremental insurance cost is devoid of said operational factor; and

preparing billing for the customer from the contracting company based on at least said first and said second incremental insurance costs.

31. (Currently Amended) The method of claim 30, further comprising having an underwriting entity provide the operator with a charge for an insuring ~~said~~ the motor vehicle, based on said first and said second incremental insurance costs ~~cost~~, for said given incremental time period.

32. (Currently Amended) The method of claim 30, wherein determining said first ~~an~~ incremental insurance cost comprises using a cost calculation system and a cost lookup database on the motor vehicle having actuarial information, in addition to said operational factor ~~recorded information~~.

33. (Currently Amended) The method of claim 30, wherein monitoring ~~an~~ said operational factor of ~~said~~ the motor vehicle comprises monitoring at least one of the group of variable comprising:

a speed of ~~said~~ the motor vehicle;

a geographic location of ~~said~~ the motor vehicle;

an acceleration of ~~said~~ the motor vehicle; and

a deceleration of ~~said~~ the motor vehicle.

34. (Currently Amended) The method of claim 33, further comprising using an external location identification system for assisting in determining [[a]] said geographic location of ~~said~~ the motor vehicle.

AMENDMENTS TO THE DRAWINGS

The attached "Replacement Sheet 2/2" of drawings includes changes to Figure 2. The attached "Replacement Sheet 2/2," which includes Figure 2, replaces the original sheet including Figure 2.

Attachment: Replacement Sheet 2/2

REMARKS

Claims 1, 4, 5, 9, 10, 14, 15, 16, 19, 20, 23, 24 and 28 – 34 are now pending in the application. Claims 1, 4, 5, 14, 15, 16, 20, 23, 24 and 28 – 34 have been amended. Support for amendments can be found throughout the Application as originally filed and therefore no new matter has been added. Claims 2, 3, 6, 7, 8, 12, 13, 17, 18, 21, 22, 25, 26 and 27 have been canceled without prejudice to or disclaimer of the subject matter contained therein. The Office is respectfully requested to reconsider and withdraw the rejections in view of the amendments and remarks contained herein.

CONTACT WITH THE EXAMINER

Applicant thanks the Examiner for the courtesies extended during multiple telephonic conversation including the conversation on October 9, 2007. The undersigned, the Examiner and Examiner Joseph Thomas took part in the conversation. The claims and references of record were discussed. No formal agreements were reached.

DRAWINGS

The drawings stand objected because reference numeral 18 is duplicated in Figure 2 on Drawing Sheet 2/2. Applicant has attached revised drawings for the Office's approval. In the "Replacement Sheet 2/2," EXTERNAL LOCATION INDENTIFICATION SYSTEM was designated with reference number 18 but has been changed to reference number 20 in the replacement sheet 2/2 attached herewith.

REJECTIONS UNDER 35 U.S.C. § 102 AND 103

Claims 1, 13-14, 16, 27-28, 30-31 and 33 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Nakagawa et al. (U.S. Publication No. 2002/0128882, Nakagawa). Claims 2-6, 9-10, 15, 17-20, 23-24, 29, 32 and 34 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nakagawa in view of McMillan et al. (U.S. Pat. No. 5,797,134, hereinafter McMillan). Claims 7-8, 11-12, 21-22 and 25-26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nakagawa in view of McMillan and further in view of Wright (U.S. Pat. No. 6,052,466, hereinafter Wright). These rejections are respectfully traversed.

Applicant has amended Claims 1, 16 and 30 and respectfully submit that Nakagawa, McMillan, Wright or any of the references of record do not disclose, teach suggest the invention as defined in the Claims.

For example, Claim 1 recites, in part, deriving a first cost increment by evaluating at least the location information, the vehicle performance information and a pricing database. The deriving of the first cost increment is performed on the vehicle. Claim 1 further recites transmitting the first cost increment from the billing transmission system to the contracting company. The first cost increment is devoid of the location information and the vehicle performance information.

In a further example, Claim 16 recites, in part, the computation device is configured to provide access for the customer outside of the vehicle to the first cost increment prior to the billing of the customer by contracting company and wherein the access for the customer outside of the vehicle to the first cost increment is adapted to permit the customer to alter driving habits to adjust a second cost increment.

In yet another example, Claim 30 recites, in part, determining a first incremental insurance cost with the recorded information for the motor vehicle related to a given incremental time period and transmitting the first incremental insurance cost to the contracting company. The first incremental insurance cost is devoid of the operational factor. Claims 30 further recites providing access for the customer outside of the motor vehicle to the first incremental insurance cost prior to the contracting company billing the customer such that the providing access to the first incremental insurance cost is adapted to permit the customer to alter driving habits to adjust a second incremental insurance cost.

Nakagawa, in contrast, provides that any factor that adjusts the cost of the vehicle insurance is routinely shared and sent to the billing company. For example, car insurance company 2 calculates the car insurance premiums based on information sent by radio communication from car 1 and information sent from contract repair factory 3. For example, when a user has properly installed safety equipment in car 1, drives car 1 safely, and properly maintains and manages car 1 at contract repair factory 3, car insurance company 2 assumes a reduction in any insurance that may have to be paid out for car 1. Therefore, the insurance premiums payable for car 1 are discounted. Conversely, if the user 1 has not properly installed safety equipment in car 1, does not drive safely, and does not properly maintain or manage car 1, car insurance company 2 assumes an increase in any insurance that may have to be paid out for car 1. Therefore, the car insurance premiums payable for that car are increased. Data relating to the car insurance premiums after any discount or increase has been applied is sent via radio communication from car insurance company 2 to car 1. The received data

relating to the car insurance premium is displayed so that it is visible to the user of car 1. *See Nakagawa at Para. 50*

Even beyond safety measures and car information, the system in Nakagawa can even use an air analyzer or breath tester to detect whether or not a user has consumed alcohol and the levels consumed. The operating status detection means 7 also includes various sensors for collecting information relating to the operating status of car 1. All of this is reported back to the billing company.

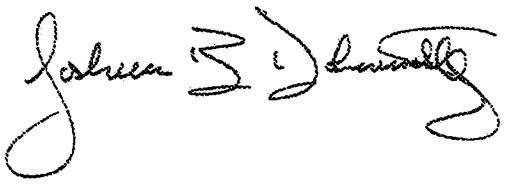
Wright and McMillan only provide for the gathering of various pieces of vehicle information that is otherwise sent back to the billing company. *See, e.g., Wright at Col. 3, Ln. 7-19 and McMillan at Col. 6, Ln. 58-62.*

For at least the above reasons, Applicant respectfully submits Nakagawa, Wright, McMillan or any other reference of record do not disclose teach or suggest the invention as defined in Claims 1, 16 and 30. As such, Claims 1, 16 and 30 should be in condition for allowance. Claims 4, 5, 9, 10, 14, 15, 19, 20, 23, 24, 28, 29 and 31 – 34 depend from Claims 1, 16 and 30 directly or indirectly and should be allowable for at least the above reasons.

CONCLUSION

It is believed that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Office reconsider and withdraw all presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding Office Action and the present application should be in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is always invited to telephone the undersigned at (248) 641-1600.

Respectfully submitted,



Dated: October 25, 2007

By: _____
Joshua B. Dobrowitsky
Reg. No. 51, 288

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600

MDE/JBD/kp

Title: SYSTEM FOR CHARGING FOR AUTOMOBILE INSURANCE
Inventor: Rodney B. Kendrick
Atty. Ref.: 7784-000652

REPLACEMENT SHEET 2/2

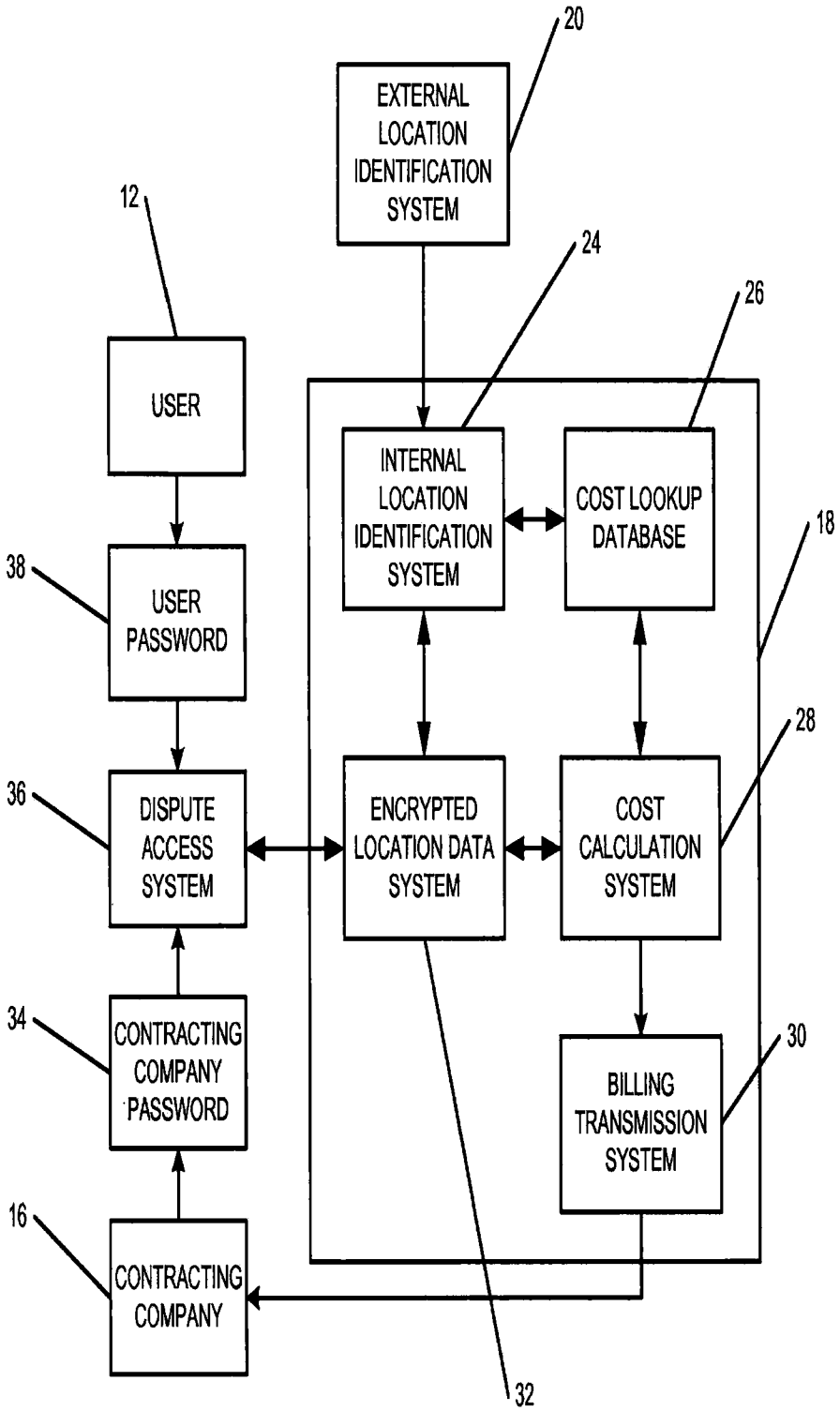


FIGURE 2